CARLOS DOMINGO

PRÓLOGO DE JUAN MARÍA NIN GÉNOVA

Todo lo que querías saber sobre BITCOIN, CRIPTOMONEDAS Y BLOCKCHAIN y no te atrevías a preguntar

Índice

Gracias por adquirir este EBOOK

Visita **Planetadelibros.com** y descubre una nueva forma de disfrutar de la lectura

---

¡Regístrate y accede a contenidos exclusivos!

Primeros capítulos
Fragmentos de próximas publicaciones
Clubs de lectura con los autores
Concursos, sorteos y promociones
Participa en presentaciones de libros

PlanetadeLibros

Comparte tu opinión en la ficha del libro
y en nuestras redes sociales:

Explora **Descubre** **Comparte**

CARLOS DOMINGO

TODO LO QUE QUERÍAS SABER SOBRE BITCOIN, CRIPTOMONEDAS Y BLOCKCHAIN, Y NO TE ATREVÍAS A PREGUNTAR

¿Ha llegado el dinero digital para quedarse definitivamente? ¿Es la blockchain la próxima revolución tecnológica? ¿Cómo va a afectar en nuestras vidas la llamada criptoeconomía?

Casi no queda nadie que no haya oído hablar del bitcoin, las criptomonedas y la blockchain. Sin embargo, continúa siendo un universo sobre el que se mantienen demasiados mitos y que provoca muchas dudas y posiciones encontradas.

Carlos Domingo, una de las voces más autorizadas en esta materia y con un discurso comprensible y bien documentado, arroja luz sobre un tema que cada vez más nos afecta a todos. Desde el convencimiento de que estamos ante una auténtica disrupción, estas páginas nos acercan a la historia del bitcoin y otras criptomonedas de nueva generación y al enorme potencial de una tecnología que va a transformar numerosas industrias y revolucionar el sistema financiero.

A mi mujer Belinda Galiano, por la paciencia que tiene con mis locuras. Y por darme a mis hijos Olivia, Adrián y Mara, lo mejor de mi vida.

PRÓLOGO

LA BATALLA DE LAS IDEAS Y LOS CONCEPTOS TRAS LAS CRIPTOMONEDAS

Es propio de tiempos de cambio acelerados: los avances llegan sin anunciarse. O, mejor dicho, cuando se anuncian es porque ya se están aplicando. Lejos quedan otras etapas en las que íbamos teniendo noticia escalonada sobre los progresos en tal o cual técnica que nos permitiría disfrutar en pocos años de telégrafos, teléfonos, ordenadores personales, Internet o móviles inteligentes. Así fue durante la primera y la segunda Revolución Industrial, también durante los primeros años de las «puntocom»,las redes sociales y la digitalización.

Pero la realidad dinámica de nuestros días nos habla, por poner un ejemplo, de la edición genómica a través de sus éxitos reales, no de sus expectativas de futuro; y lo mismo ocurre con avances científico-técnicos relacionados con la comunicación, la ingeniería aplicada o en ocupaciones menos venturosas, como la carrera armamentística en la que la inteligencia artificial permite a los guerreros no humanos independizar sus decisiones de acción. El futuro ya no es un vaticinio, sino el día a día, a veces el ayer.

En esta concepción temporal del progreso se incardina eso que se ha dado en llamar criptomonedas, que por ser la más conocida y extendida, el bitcoin representa ante el gran público con su nombre, sin ser la única. A su vez, la poderosa luz mediática de esta criptomoneda deja en la sombra la tecnología revolucionaria que la sostiene: la blockchain o cadena de bloques. No es tan sorprendente que no sepamos qué son, sino que no sepamos qué son cuando ya son parte de la rutina de nuestro sistema. Han avanzado rápido y en silencio.

De iluminar esa zona oscura se encarga con énfasis didáctico y rigor técnico Carlos Domingo en el libro que el lector tiene entre sus manos. El autor desgrana su diagnóstico y no esconde su pronóstico: «Tengo claro que esto es el futuro», nos dice.

La aceleración del tiempo histórico ha sido tal que nos vemos impelidos a asumir conceptos nuevos, a normalizarlos en nuestra reflexión privada y conversación pública, sin saber realmente de qué estamos hablando. Conviene detenerse a pensar en la realidad y la potencialidad de las criptomonedas y la tecnología que la sustenta. Además, también es razonable pensar que el público general que lo asumirá y lo disfrutará —o padecerá, si se hace un mal uso—, necesita formarse, saber más y mejor de todo lo que implican estos cambios. La responsabilidad financiera individual es indisociable de la autoformación activa, y este libro, claro, directo y riguroso sobre qué es, qué cambios ha producido y cuáles puede producir la irrupción de las criptomonedas, facilita esta tarea.

Pero no es solo la propia aceleración de ese tiempo histórico la que hace que observemos los cambios con cierto vértigo y actitud recelosa por la exigencia de permanente puesta al día. Por un lado, no hace tanto que hemos sufrido una crisis tan severa que nos llevó a una gran recesión, de modo que los anticuerpos están en guardia ante cualquier innovación del sector financiero y bancario, o todo aquello tangencialmente relacionado con ellos. Por otro, la psicología cognitiva lleva años señalando los fundamentos neurológicos de las resistencias al cambio. Existen inercias que no solo es necesario vencer con argumentos técnicos irrefutables, sino con persuasión y pedagogía y finalmente con la práctica. Este libro también contribuye a ello.

¿Qué hace del bitcoin en particular, y de las criptomonedas en general, algo tan disruptivo? ¿Por qué tantos analistas, líderes políticos y de opinión mediáticos nos alertan de su naturaleza tóxica y su aspecto de burbuja? Podríamos pensar que existen problemas con los fundamentos tecnológicos, pero como bien explica Domingo, hay pocas herramientas tan afinadas como la blockchain. Además, su aplicación ya va, y seguirá yendo, mucho más allá de las criptomonedas. Es un subyacente de primera. ¿Es su escasa consistencia económica? Tampoco. Las criptomonedas se basan, como las monedas de curso oficial, en la confianza. Desde que Richard Nixon decretara la ruptura del patrón dólar-oro allá por 1971, no ha existido ningún respaldo para nuestros intercambios, y nuestra reserva de valor, distinto al de la promesa del Estado de sustentar las monedas con las que se ejecutan, dinero fiat. Esto es, se basan en la confianza, y algunas veces más bien en la fe en el recto funcionamiento de las instituciones públicas.

Las criptomonedas no son distintas en esto por más que la minería del bitcoin lleva aparejado un coste que lo puede asimilar a la del oro, aunque sí parten de una desconfianza previa: la que sienten —no solo ellos, sino la gran mayoría de

los usuarios— hacia las autoridades bancarias públicas y privadas y el monopolio estatal de la emisión de moneda. Y, bien pensado, no es una desconfianza caprichosa. ¿Por qué confiar en unos reguladores que no anticiparon —si es que no alimentaron— la crisis financiera? Por resumir, podemos decir que, en aparente paradoja, las criptomonedas se sustentan en la confianza —como el resto de monedas—, pero nacen de la desconfianza en los emisores y los gestores de la política monetaria. También en cierto valor añadido —su coste de fabricación— superior al mero apunte contable o el físico del papel.

Y entramos aquí en el gran escollo que deberán vencer las criptomonedas y en lo que explica la reacción, a veces sobreactuada, en su contra. Como hemos visto, las criptomonedas suponen una innovación tecnológica, de la herramienta, pero no de su finalidad; esto es, el intercambio de bienes y servicios y la reserva de valor. Sí son, en cambio, un competidor nuevo en un entorno dominado por monopolios de bancos centrales con varios siglos de antigüedad. Las criptomonedas suponen una innovación técnica para facilitar operaciones económico-financieras, pero también son una disrupción jurídico-política que afecta al núcleo esencial del poder económico y monetario del orden westfaliano del Estado-Nación. De ahí la reacción cauta y, a veces, visceral en su contra desde tantos sectores. El fin del monopolio de la emisión de moneda por parte de los Estados es un problema político y jurídico, no tanto monetario o económico, mucho menos tecnológico.

Quedan incógnitas por resolver, pero no parece que vayamos a tardar mucho en despejarlas dado el ritmo de avances y cambios. En ese reto jurídico-político que mencionamos, está presente su utilización para fines delictivos en eso que se ha dado en llamar la *Deep Web* o Internet profunda. No son, en cualquier caso, problemas exclusivos de las criptomonedas. No obstante, habrá que prestar atención a este potencial uso nocivo del bitcoin que se ha constituido en el principal argumento para exigir su sometimiento al viejo esquema.

Queda por saber si será necesaria algún tipo de regulación. La propia naturaleza libertaria de las criptomonedas nos hace preguntarnos si funcionará eso que el economista Friedrich Hayek llamaba —aunque ya el taoísta Zhuangzi lo mencionara en el siglo IV a. C.— «orden espontáneo» y, por lo tanto, prosperará con independencia de cualesquiera regulaciones. O si operará la positiva «destrucción creadora» que Schumpeter veía en los procesos disruptivos. Será interesante ver de qué lado de la balanza política se inclinarán las criptomonedas. Porque frente a ese «orden espontáneo» y esa «destrucción

creadora» de raíz liberal que se acaba imponiendo de abajo arriba frente al caos, la actual mayoría defiende que es necesario imponer una regulación normativista e intervencionista de arriba abajo. El dinero fiat, monopolio del Estado, librará una batalla casi final con las criptomonedas.

Es en esa batalla política de ideas y conceptos —y no de técnica, eficacia y oportunidad— donde se decidirá el futuro de unas criptomonedas, cuyo potencial beneficioso quedan magistralmente explicadas en este libro tan necesario.

JUAN MARÍA NIN GÉNOVA
Consejero Delegado del Banco Sabadell (junio 2002-junio 2007)
Consejero Delegado de CaixaBank (julio 2011-julio 2014) T_

INTRODUCCIÓN

LA SIGUIENTE REVOLUCIÓN TECNOLÓGICA

El bitcoin, las criptomonedas y la blockchain están de moda. O al menos, en boca de todos. Hoy por hoy me da la sensación de que ya no queda casi nadie que no haya oído hablar, aunque sea coloquialmente, de la famosa moneda digital o la nueva tecnología disruptiva que va a revolucionar el mundo. Además, a las personas nos gusta, sobre todo si algo es tan novedoso, lanzarnos a opinar enseguida sobre las cosas que irrumpen en nuestras vidas con tanta fuerza. De manera que, día sí y día también, nos encontramos en el debate público, ya sea con mayor o menor conocimiento de causa, conversaciones y pronósticos en torno al llamado dinero digital, el bitcoin y otras criptomonedas, y en torno a la tecnología que lo sustenta, la blockchain —lo cual no deja de ser un tanto sorprendente por cuanto entramos en un territorio técnico y económico un tanto complejo para la gran mayoría—.

Lo cierto es que estamos todos manejando una serie de conceptos novedosos y en última instancia bastante complejos que todavía distan mucho de tener unos cimientos bien asentados en nuestros mercados, pero que conforman desde ya un atractivo marco de actuación no exento de controversia. Tal es así que, a la que nos podemos referir como criptoeconomía, la están cortejando ya muchos desde una proliferación de miradas de muy diversa índole y posicionamientos completamente antagónicos.

Esa disparidad de opiniones es fácil de comprobar echando un vistazo a Internet. Tampoco es necesario indagar demasiado, ya que estamos siendo constantemente bombardeados con noticias y artículos al respecto que, por un lado, nos dibujan un prometedor universo de posibilidades, pero por otro nos advierten de que todo esto no es sino una burbuja o un fraude —tal y como afirmó, haciéndose enseguida famosa esta interpretación, el consejero delegado de J. P. Morgan, Jamie Dimon. Más adelante se arrepintió públicamente de

haberlo dicho—, una suerte de esquema Ponzi que va a terminar estallando, de manera que los bitcoins y otras criptomonedas, como algo puramente especulativo, van a dejar de tener el más mínimo valor.

El entusiasmo por parte de los primeros es significativo, rozando lo religioso: nos tratan de demostrar que esta no solo es la mejor inversión financiera que podíamos haber hecho en los últimos años, sino que todo este fenómeno que ahora apenas empieza a emerger representa la siguiente revolución tecnológica por llegar comparable a la propia irrupción de Internet, la nueva Internet del valor y la nueva Internet descentralizada. Para sus defensores, va a ser capaz de transformar no solo el dinero, la industria financiera y los mercados de capitales tal y como los conocemos en la actualidad; además, va a dar lugar a una nueva Internet descentralizada que rete el control vigente de la misma que tienen los grandes actores como son Google, Amazon, Facebook o Apple.

Frente a ellos, sin embargo, no dejan de alzarse voces agoreras, y no son pocos quienes se dedican a levantar obstáculos para limitar un desarrollo sin trabas de todo lo que concierne a la criptoeconomía o a las plataformas públicas de blockchain.

De manera que no cabe sino hacerse la gran pregunta: ¿quién lleva razón? No voy a andarme con rodeos: yo tengo claro que esto es el futuro. Seguramente a mucha gente le atraerá la parte especulativa de la cuestión como vía para enriquecerse, dado el asombroso crecimiento de valor que, a pesar de ciertos altibajos y una gran volatilidad, ha experimentado el bitcoin y otras criptomonedas en menos de diez años de existencia. Reconozco que la parte de inversión financiera que este asunto conlleva es, sin duda, un terreno interesante sobre el que reflexionar y que conviene también abordar, por lo que no la dejaré de lado; sin embargo, lo que a mí me fascina especialmente es el potencial disruptivo que trae consigo la tecnología que hay detrás y su capacidad para transformar la economía del futuro.

Como veremos, las plataformas de blockchain públicas nos traen el protocolo que nos faltaba para poder trasmitir valor de forma descentralizada y segura por Internet. Gracias a esto, cualquier actor que hoy por hoy intermedia con valor como modelo de negocio, desde los bancos que nos permiten mover dinero de una cuenta a otra, a los notarios que nos garantizan la validez de un contrato, o a alguien como Uber o Airbnb que nos intermedian para proveernos de transporte o alojamiento, son susceptibles de ser disrumpidas y reemplazadas por su versión descentralizada en la blockchain, donde la propia plataforma provee de

esa seguridad y confianza que hoy nos dan los intermediarios actuales y que, por supuesto, nos cobran por ello.

Entramos en la era de la criptoeconomía, pero para comprenderla es fundamental entender primero lo que es el bitcoin, puesto que se trata de la primera criptomoneda que apareció y la que proporcionó el sustento tecnológico —la blockchain— que habrá de transformar radicalmente las cosas.

Por eso, con estas páginas lo que pretendo es, en primer lugar, ofrecer un acercamiento conceptual al bitcoin, a su historia y a todos sus derivados, para terminar por sumergirnos en el campo de la innovación tecnológica con la blockchain, y en cómo esta tecnología está transformando ya el mundo financiero, y cómo puede disrumpir en el futuro la economía.

La idea del libro surge de una charla que di, por invitación de Julio Alonso —el fundador y CEO de Weblogs— en el evento de su publicación *Xataka* en Madrid en diciembre de 2017, y que llevaba el mismo título de este libro. El vídeo de la misma en YouTube —https://www.xataka.com/criptomonedas/bitcoin-blockchain-y-criptomonedas-explicado-de-forma-sencilla-y-en-video— tuvo más de 45 000 visitas y en general comentarios muy positivos de mucha gente que le pareció que se explicaba todo este nuevo mundo de manera sencilla y accesible. Eso me hizo ver la necesidad de acercar estos temas a una audiencia no necesariamente técnica o financiera. En cierto modo, este libro es la versión escrita y más detallada de esa charla.

Admito que yo mismo no terminaba de entender hasta muy recientemente por qué se hablaba de todo esto como algo tan revolucionario. Llevaba prestando atención a estos temas desde el año 2015, pero no fue hasta principios de 2017, con el crecimiento de otra cuestión muy relacionada con la criptoeconomía como son las ICO —*Initial Coin Offering*, una nueva y revolucionaria forma de financiación de start-ups usando blockchain, de la que también tendremos espacio para explicar en qué consiste—, cuando algo cambió en mi percepción.

Concretamente, ocurrió cuando me encontré con mi amigo Brendan Eich, inventor de famoso lenguaje de programación Web Javascript y fundador de Mozilla, la compañía que creó el navegador de Internet Firefox, en febrero de 2017 en el Mobile World Congress en Barcelona. Durante esa reunión me describió cómo iba a emitir su propia criptomoneda o token para su nuevo negocio Brave. Luego llevaría a cabo una de aquellas primeras ICO, seguramente la primera de las importantes, donde consiguió en solo treinta segundos un total de 35 millones de dólares de financiación para su proyecto.

Esa experiencia me permitió comprobar algo fundamental que me hizo empezar a ver la luz, porque lo que se me estaba mostrando era una nueva Internet que no solo transfería contenidos e información, sino también valor, y aquí residía el quid de la cuestión.

La blockchain nos permite movernos de la Internet de la información a la Internet del valor, y esta es una idea fundamental en la que focalizaré la atención en los próximos capítulos. Porque transmitir valor de forma descentralizada, segura y con confianza es completamente revolucionario y con potencial para transformar todo el sistema financiero tal y como lo conocemos hoy, y por extensión otros muchos sectores de actividad y la economía global.

Lógicamente, instituciones bancarias, notarías y los agentes que se dedican o participan de la intermediación financiera no terminan de ver con buenos ojos esta transformación, puesto que viven de una función, la intermediación, que esta tecnología elimina.

Tendrán que adaptarse. Ya pasó con las empresas de telecomunicaciones cuando, entre otras transformaciones, se vivió cómo WhatsApp limitó el envío de los SMS—con los que las compañías de telefonía obtenían grandes beneficios — a algo residual, o Skype hizo lo mismo con las llamadas internacionales. Precisamente, este era el sector en el que yo trabajaba, por lo que he sido testigo en primera línea de lo que pasó, y creo poder prever lo que habrá de pasar ahora en otros sectores ante una disrupción parecida.

Recuerdo hace no mucho cuando, ahora que resido fuera de España, quise comprar una nueva casa por la zona de Castellón de la que procede mi mujer, una región que solemos visitar con frecuencia. Pues bien, realizar esa compra desde el extranjero y lidiando con el sistema bancario tradicional, fue un proceso repleto de incomodidades, tiempo perdido y gastos desorbitados e innecesarios en comisiones, precisamente porque todavía no es extensivo un uso de transferencia de valor que nos permite, ya en la práctica, el nuevo escenario del dinero digital y la tecnología blockchain.

Las transferencias internacionales de dinero son lentas y costosas —transferir dinero de un país a otro tarda tres días cuando el dinero ni siquiera se mueve físicamente—, hay pagos que solo se te permiten hacer mediante cheque, se requieren notarios para muchas operaciones en las que, además, exigen estar presente… Es arcaico. Esta experiencia personal reciente me parece muy ilustrativa y es probable que en ella la mayor parte de los lectores encuentren equivalencias con respecto a circunstancias propias vividas. Se trata de procesos incómodos, lentos y muy costosos que hoy no deberían ser necesarios.

No tiene sentido que en el siglo XXI sigamos todavía haciendo las transacciones financieras como las estamos haciendo, cuando podríamos mandar dinero encriptado garantizado, usando blockchain de forma absolutamente segura en décimas de segundo. Por eso, lo que resulta revolucionario es que ese proceso de intercambio de valor que emprendí al comprar una casa en Castellón, podría haberse hecho de manera completamente segura, automatizada e instantánea, y sin costes de transacción. Las blockchains públicas son la siguiente revolución tecnológica que va a transformar industrias que hasta ahora no se habían visto afectadas por Internet al ser capaz de desintermediar a los actores actuales del mundo financiero, reduciendo los costes y la fricción que en la actualidad experimentamos en cualquier transacción.

Al final de este libro veremos con detalle cómo todo esto se podría haber hecho con criptomonedas, blockchain y los llamados contratos inteligentes —conocidos también por su nomenclatura en inglés *smart contracts*— de forma rápida y barata, y eliminando a los intermediarios tradicionales de estas operaciones —bancos y notarios, como hemos dicho—.

Entiendo que en esta introducción estoy presentando seguramente demasiados conceptos: por supuesto el bitcoin, pero también la blockchain, los *smart contracts*, las ICO, etc., que exigen explicaciones más detalladas en los próximos capítulos. Los presento ya porque quiero dejar claro desde aquí que, aunque a algunos quizás no les haga gracia la idea, el mundo va a cambiar contundentemente en los próximos años gracias a una nueva tecnología disruptiva, tal y como en su día cambió con Internet o con los smartphones.

Es cierto también que nos encontramos todavía en un mercado incipiente, muy poco maduro, que arrastra problemas técnicos y lagunas legales. Las monedas digitales, aunque den tanto de qué hablar como decíamos al principio —hoy Internet y las redes sociales amplifican mucho toda cuestión novedosa—, ahora mismo las emplea solo un porcentaje mínimo de personas, pero tengamos en cuenta que también Internet en sus inicios de los años noventa apenas lo usaba nadie. El caso es que es algo que está explotando justo ahora y el camino se hace al andar; un camino que yo creo que va a trazar un recorrido apasionante, aunque no exento de incertidumbres. Apenas ha pasado una década desde que el bitcoin naciera, pero preveo que en los próximos diez años el crecimiento va a resultar espectacular, así como el calado de las transformaciones que se van a producir.

Esta mirada hacia el futuro es a la que quiero dedicar la última parte de este texto, porque no deseo limitarme a dar una explicación conceptual en torno al bitcoin y la tecnología que lo sustenta —aspectos que ocuparán los primeros

bloques del libro—. Soy consciente de que mi visión optimista no es compartida por todos, y que a muchos no les conviene el cambio o simplemente no se creen que vaya a pasar. Tampoco estoy sordo como para no oír las alertas sobre la dimensión especulativa que conlleva o sobre el hecho de ser una burbuja que va a explotar, de la falta de seguridad que existe en algunas aplicaciones y los continuos *hackeos*, de la falta de escalabilidad de estos sistemas descentralizados comparados con los financieros tradicionales, de su alto consumo energético…

Hay varios mitos en torno a la criptoeconomía que también tendremos oportunidad de evaluar más adelante, pero estoy convencido de que todo esto está aquí para quedarse y que va a cambiar muchísimas cosas, y no solo relativas al sector financiero. También cuando Internet empezó era lentísimo conectarse a la red, se hacía mediante un módem con continuos fallos de conexión, la carga de las páginas era lenta y primitiva, con contenidos mayoritariamente de texto, pero el alto valor que aportaba en muchos ámbitos hizo que la industria fuera solucionando estos problemas poco a poco hasta convertirse en lo que es hoy. Lo mismo creo, como he dicho, que va a pasar con el mundo de la criptoeconomía.

Para mí también es todo un reto después de tantos años dedicados a la innovación. En mi carrera he tenido la suerte de pasar por dos momentos decisivos en la historia de la innovación y del mundo de la tecnología moderna. Por un lado, empecé a trabajar hacia finales de los noventa al acabar mi doctorado en el momento justo en que la burbuja del dot.com estaba en plena ebullición y viví en primera persona tanto la subida —con un IPO y salida a bolsa incluida de la empresa para la que trabajaba—, como la caída de la misma, teniendo que realizar despidos y reorganizaciones para sobrevivir.

Mi siguiente paso profesional fue en el mundo de las telecomunicaciones, al entrar a Telefónica en el año 2006. Entonces fui testigo de la revolución del mundo móvil que vino de la mano de Apple y Google con el lanzamiento del iPhone en 2007 y de Android en 2008.

Ahora acabamos de atravesar otro de esos momentos clave. Creo que 2017 será recordado como el año Netscape —Netscape fue el primer navegador comercial de Internet que hubo y su salida a bolsa en 1995 se considera el principio de la era Internet— para el mundo de las criptomonedas y de blockchain. Después de más de diez años en las telecomunicaciones no podía dejar escapar el entrar en este mundo profesionalmente, y dar paso así a una tercera etapa laboral en mi carrera. Hoy por hoy me dedico en exclusiva a estos temas, habiendo logrado crear el fondo tokenizado en la blockchain más grande del mundo, SPiCE VC, así como la plataforma líder para la emisión de tokens

securitizados o tokens respaldados por activos —todos estos conceptos ya los explicaremos más adelante— llamada Securitize.

Cuando empecé mi pequeña obsesión con los temas de cripto —me referiré de forma general con la abreviatura cripto a todo este universo relacionado con las criptomonedas, tokens o blockchains públicas— hace cosa de un año —hasta el punto de dejar mi trabajo corporativo de aquel momento—, hubo quienes me dijeron que quizás me estaba volviendo un poco loco. Pero lo hice desde el convencimiento y la pasión. Por eso también siento la necesidad de explicar de la manera más comprensible posible a la gente que no tenga especiales conocimientos técnicos financieros o informáticos en qué consiste todo esto y cuál es su enorme potencial. Quiero hacer comprender por qué creo que es algo tan revolucionario el bitcoin, las blockchains, los tokens, las ICO, la criptoeconomía, la Internet del valor y el futuro descentralizado que nos espera.

Ese es el propósito de este libro. Un punto de partida que confío resulte útil, porque nos hallamos, no lo dudes, ante un área prioritaria para empezar a investigar por parte de profesionales y agentes de muy diversa índole.

PRIMERA PARTE
ORO DIGITAL

1
UNA BREVE HISTORIA DEL DINERO

Hoy en día hablamos de dinero digital con normalidad, pero habrás comprobado que se ha extendido también el uso de la expresión «oro digital» cuando la gente se refiere al bitcoin y las criptomonedas. No es gratuito ni está nada mal elegido ese término de ‘oro’, y no solo por esa connotación que tiene metafóricamente como de algo que es muy valioso, o como sinónimo de riqueza, sino también por lo que este metal precioso ha representado en la historia del dinero.

Por eso, para entender mejor lo que viene a significar el bitcoin, conviene hacer un breve recorrido por la historia del dinero que hemos citado: desde la misma Prehistoria hasta la crisis económica mundial de 2008, desde el trueque hasta el dinero digital; un trayecto que te ayudará a entender mejor la realidad de lo que representa hoy la aparición de una criptomoneda como el bitcoin.

Este recorrido histórico que quiero realizar como capítulo primero ayudará a fijar ideas y conceptos que resultarán valiosos más adelante, y nos va a permitir ver que la concepción original del dinero se ha desvirtuado de manera considerable a lo largo del tiempo, y que quizás es precisamente ahora el dinero digital el que la está recuperando. Pero vayamos poco a poco.

El dinero no ha existido siempre. Al principio se practicaba el trueque: uno producía leche porque tenía una vaca y cambiaba esa leche a un agricultor por patatas, o por cualquier otro bien que necesitara o no tuviese. Obviamente, esta no era una forma fluida de funcionar cuando las comunidades iban creciendo, y es algo que en sociedades amplias resulta muy ineficiente. Por eso, ya desde el Neolítico, en Mesopotamia, paralelamente al nacimiento de la civilización 2500 años a. C., se tuvo la idea de que debía haber algo intermedio para canjear. Es así como nació el dinero, una herramienta que permitió intercambiar, comprar y vender las cosas. Aunque, en realidad, ya desde su concepción, la moneda fue algo más, y cumplió con tres funciones fundamentales, que conviene que tengamos muy en cuenta:

— Una moneda es algo en la que puedes almacenar valor, que se cuantifica.
— La moneda, tal y como decíamos, es algo que puedes intercambiar por cosas, que te permite pagar por hacer transacciones.
— Y finalmente, la moneda es algo que sirve para referenciar: es una referencia de valor que otorga precios a las cosas.

Seguramente, la mayoría nunca nos hemos parado a pensar en estos tres conceptos que reúne toda moneda para cumplir con su función, los hemos dado por sentado, pero es importante que aquí los manifestemos expresamente porque va a ser necesario recordarlo cuando hablemos de las criptomonedas.

Pero volviendo a aquellos pastores del Neolítico que inventaron el dinero, posiblemente tampoco les resultara fácil llegar a crear una moneda que les sirviera, y es más que probable que hubiera unos cuantos ensayos fallidos. Y es que una moneda para ser realmente eficaz exige poseer unas cuantas características, pues no cualquier cosa servía para intercambiar, almacenar y ser una referencia de valor. Por eso, la moneda debía ser:

√ Escasa. Si fuera sencilla de conseguir como, por ejemplo, una piedra corriente, no tendría mucho sentido. Uno no iba a querer dar lo que ha producido o conseguido con esfuerzo por un puñado de guijarros que podría recoger en la calle.
√ Difícil de copiar. En caso contrario perdería su valor. Si la moneda elegida fuera fácilmente reproducible, cualquiera fabricaría su propio dinero, provocando una inflación galopante y la pérdida de confianza en ella.
√ Portable. Si se había de usar para intercambios en un mercado, debía poder ser transportada por uno mismo.
√ Perdurable. Si corría el riesgo de perderse por el mero paso del tiempo o porque se estropeara por las condiciones meteorológicas, no se antojaría muy eficaz.
√ Fácilmente divisible en unidades pequeñas para poder adaptarse a todo tipo de transacciones.
√ Deseable. Es decir, que apelara por sí misma el interés de una persona.

Con estos criterios —seguramente de manera inconsciente o instintiva— fueron desarrollándose las formas primitivas de dinero, siendo los metales preciosos los que fueron poco a poco ganándose el privilegio de ser considerados el objeto más adecuado. Estos metales preciosos al principio fueron valorados en

función de su peso, estableciéndose una equivalencia entre este y su valor, pero con el tiempo se fueron transformando ya en monedas acuñadas al estilo que nos resulta más familiar hoy en día, algo que se extendió de forma casi simultánea en varios lugares del mundo —desde el Oriente más próximo hasta China— hacia el año 600 a. C.

No obstante, incluso antes de estas monedas, ya habían aparecido los primitivos bancos. Puede sorprender esta cronología, pero lo cierto es que las monedas, y después los billetes, exigen una estructura burocrática previa que les conceda validez. Los primeros bancos fueron los propios palacios o templos en Mesopotamia y Egipto, recintos que estaban muy bien custodiados y en los que se almacenaban los metales preciosos y otras materias primas, extendiéndose un recibo a cambio del depósito —un recibo que ya servía para realizar transacciones con terceras partes—.

Los billetes de papel nacieron en China alrededor del siglo VIII d. C., aunque después —en el XV— abandonaron esta forma de dinero durante centurias. En Europa los billetes no llegaron hasta el XVII —Suecia fue el país pionero—, fruto del fuerte incremento de la actividad económica y comercial, la cual demandaba una provisión de dinero superior a la que podían ofrecer los metales.

Con el papel se dio un paso más en la evolución del dinero, ya que la moneda empleada dejaba de tener un valor intrínseco en su soporte físico, y lo que importaba era el respaldo que tenía detrás por parte de sus emisores —finalmente los Estados, aunque inicialmente también hubo emisores privados—.

A partir de este momento en que se hace extensivo el empleo de billetes que vienen avalados por los Estados, se va instaurando el hecho de que cada país termine contando con su propia moneda nacional, que es emitida en una cantidad que viene respaldada por sus reservas de oro. Nace así el patrón oro, que fue inicialmente modelizado por el famoso filósofo —también economista— británico David Hume a mediados del siglo XVIII, y que se consolidó en los acuerdos de Bretton Woods en 1944, justo después de la Segunda Guerra Mundial.

En aquel momento se acordó adoptar un patrón oro según el cual Estados Unidos debía mantener el precio del oro en 35 dólares por onza, y se le concedió la facultad de cambiar dólares por oro a ese precio sin restricciones ni limitaciones.

Al mantenerse fijo el precio de una moneda —el dólar—, los demás países debían fijar el precio de las suyas con relación a aquella, y de ser necesario,

intervenir dentro de los mercados cambiarios con el fin de mantener los tipos de cambio dentro de una banda de fluctuación del 1 %.

El patrón oro es, por lo tanto, un mecanismo que fija la emisión de monedas y billetes en un país en función de la cantidad de oro que posea, lo cual resultaba muy útil. Cuando los billetes vinieron avalados por una autoridad central, se evitaba el riesgo de bancarrota; pero existía otro, el de la inflación, para el caso en que un país imprimiera demasiado dinero. Y eso es lo que evitaba el patrón oro, una idea que no deja de estar inspirada en los primitivos tiempos en los que la moneda emitida dependía de la cantidad de metal precioso disponible, estableciéndose así un límite.

En el ámbito doméstico, el patrón oro mantiene la cantidad de dinero en circulación más o menos estable, y evita la inflación; y en el internacional, permite fijar las tasas de cambio entre monedas, concediendo, además, una estabilidad a las mismas.

Esta fórmula funcionó muy bien durante mucho tiempo, mientras los países cumplieron con la regla, pero en el siglo XX sufrió diversos varapalos —la Primera Guerra Mundial, la Gran Depresión, el colapso de los acuerdos de Bretton Woods…—, lo que provocó que los Estados se fueran saltando el patrón establecido y emitieran más dinero del que les correspondía.

Al final, en 1971 —el año que yo nací—, murió definitivamente el patrón oro, algo que fue oficialmente anunciado por Richard Nixon. Los dólares dejaron de tener una correspondencia con el oro depositado en la Reserva Federal norteamericana, que es lo mismo que decir que la moneda dejaba de tener un valor que fuera sustentado por nada. Es en este momento que se pasa del llamado dinero fiduciario al llamado dinero fiat —del latín *fiat* que quiere decir ‘que así sea’—, un término que se usa mucho en el mundo cripto para referirse a las monedas no cripto como el dólar o el euro.

Es importante entender esto porque es un punto de inflexión fundamental: el dinero fiat, ya sea el dólar, la peseta —en aquel momento— o el euro —ahora— pasa a tener el valor que nosotros queramos concederle o que los gobiernos le concedan por decreto, pero sin ninguna relación con reservas físicas. Si lo aceptamos como medio de pago —como almacén de valor, como medio de intercambio, como referencia de precio—, será válido; si no lo aceptamos —como ocurre ahora con la peseta o con cualquiera de las monedas nacionales de los países de la Unión Económica y Monetaria europea—, dejará de tener valor, puesto que detrás de nuestros euros o dólares no hay ningún sustento como en su

momento hubo con el oro, y valdrá solo si todos estamos de acuerdo en que valga.

De manera que desde 1971 el patrón oro ha sido sustituido por el dinero fiat, es decir, el que se basa, como decimos, en la «fe o confianza de la comunidad». No posee valor intrínseco, y su valor se asienta enteramente en la confianza que nos ofrezca su emisor y en el acuerdo común. Este concepto es muy importante porque una de las críticas habituales sobre las criptomonedas es que no tienen valor intrínseco. Aunque como vemos, tampoco lo tienen el dólar o el euro.

Renunciar al patrón oro fue el primer paso de un proceso que ha terminado desvirtuando la concepción original de lo que era el dinero, algo que ha terminado de confirmarse en la reciente crisis económica mundial de 2008. Insisto en esta idea porque tiene mucho que ver con el debate que mantengamos en torno a las criptomonedas un poco más adelante.

Una vez que el patrón oro fue abandonado y que, por lo tanto, se podían emitir tantos billetes como se quisiera, los bancos centrales —la Reserva Federal en Estados Unidos, el Banco Central Europeo, etc.— asumieron un rol mucho más activo y relevante en la política monetaria de cada moneda. La política monetaria de una moneda —y veremos después que las criptomonedas también la tienen— es la disciplina económica que controla la cantidad de dinero en circulación para garantizar la estabilidad de los precios y el crecimiento económico. Básicamente tira de dos palancas: la cantidad de dinero que se emite —política monetaria expansiva cuando se aumenta— o que retira de circulación —política monetaria restrictiva— y los tipos de interés. Para incidir en estas palancas los bancos centrales usan herramientas como la reducción del coeficiente de caja de los bancos —para que puedan prestar más dinero o comprar o vender deuda pública para incrementar— o la reducción de la cantidad de dinero en el mercado.

Enseguida llegaremos a esa crisis económica mundial y abordaremos la cuestión, pero cerremos antes este breve recorrido por la historia del dinero, pues todavía presenta algunos hitos dignos de mención. Sobre todo, hay que citar la aparición de los cheques y las tarjetas de débito y crédito, que permiten realizar los pagos sin llevar el dinero encima. Nacieron en los años ochenta del siglo pasado y se popularizaron con rapidez, estando su uso, como sabemos, completamente extendido.

Todavía no hablamos de dinero digital, pero sí del empleo de tecnología electrónica para poder usar un dinero que nos pertenece, pero que no necesitamos llevar encima. Y eso es ya un acercamiento al *e-money*,que nos permite también, a través de Internet, realizar pagos telemáticos sin necesidad de

mostrar tampoco nuestro cheque o tarjeta a la otra parte, realizándolos desde nuestro ordenador o a través del móvil. Pero estas fórmulas, por supuesto, se siguen aplicando a la transferencia del dinero fiat y no se pueden considerar como dinero nativo digital.

Es así como llegamos al punto actual y a la irrupción de las criptomonedas descentralizadas no emitidas por ningún banco central.

Nos conviene recapitular: estamos en un momento en el que funcionamos todos con un dinero que no tiene valor intrínseco, no respaldado por ningún patrón oro, que puede emitirse físicamente en monedas y billetes, que tienen validez para ser empleado en soporte físico, aunque luego también hay formas de emplear ese dinero fiat electrónicamente, sin necesidad de llevarlo encima.

Esta es la realidad actual, y ya lo era en el año 2008, cuando estalló la última gran crisis económica. Pues bien, yo creo que a partir de ese momento se inició una nueva etapa en la historia del dinero: la del dinero digital, de las criptomonedas, de la criptoeconomía, en definitiva. Y nuestro breve repaso histórico debe terminar aquí, porque lo que viene ahora todavía lo estamos escribiendo, y no es historia, sino futuro. Sin embargo, antes de dar por concluido el capítulo, quiero hacer notar el instante crucial en el que lo interrumpo para dar paso a la nueva etapa del dinero digital. Si hemos llegado justo hasta el momento de la crisis económica de 2008 es por motivos bien significativos y no solo por resaltar una fecha clave en la historia financiera y económica reciente.

La crisis económica sacó a la luz especialmente la vulnerabilidad de nuestros sistemas bancarios y la desconfianza creciente de la población en las instituciones financieras. A lo que hay que añadir la pérdida de riqueza y beneficios sociales que la gente padeció, fruto de los ajustes económicos que debieron emprenderse por parte de los Estados.

Hubo también otras consecuencias en relación con las políticas monetarias. Ante la crisis económica lo que hicieron en buena medida los bancos centrales en muchos países fue bajar los tipos de interés a casi un 0 % y emitir más dinero —políticas que resultaban inflacionarias y devaluaban su valor, obviamente—.

Estas políticas monetarias continúan hoy. De marzo de 2015 a marzo de 2016, el Banco Central Europeo ha impreso 60 000 millones de euros por mes con un total de 700 000 millones de euros nuevos emitidos en un intento de renergizar las economías europeas después de la crisis. Este es, por lo tanto, otro factor que subraya la distorsión de la concepción original de lo que es el dinero que citábamos antes. Uno de los rasgos característicos del dinero es que sea escaso y

limitado, pero en la práctica ya deja de serlo cuando los bancos centrales pueden emitir lo que quieran en situaciones de emergencia —o no tan de emergencia—, como así se ha hecho desde la crisis económica.

Esta realidad hace que no se nos antoje del todo casual, que justo en el mismo año en el que estalla la crisis económica, que se practican políticas monetarias que atentan contra la idea de la escasez del dinero, que se extiende la desconfianza en las instituciones bancarias y financieras —e incluso en el valor del dinero—, y que la gente ve peligrar sus ahorros y su riqueza, sea cuando nace el bitcoin, que habría de convertirse en la primera moneda digital en funcionamiento.

En noviembre de 2008, con la crisis económica internacional que acababa de explotar, el mundo se volvió a revolucionar. Había llegado el momento de ver nacer al protagonista de este libro.

2
¿QUÉ ES EL BITCOIN?

2008: ESTALLA LA CRISIS, NACE EL BITCOIN

Que precisamente en el año 2008 viera la luz la formulación de la nueva moneda digital, se antoja, como hemos dicho, muy poco casual. Existen varias evidencias de que este *timing* no fue nada caprichoso.

La crisis explotó en Estados Unidos al principio como una crisis hipotecaria y pronto se extendió al resto del mundo como un tsunami que haría temblar los cimientos de todo el sistema financiero y haría desaparecer o ser absorbidas entidades financieras tan importantes como Lehman Brothers —que quebró— o Merrill Lynch —que fue comprada por el Bank of America a precio de saldo—.

Como decíamos en el capítulo anterior, algo así provocó, como no podía ser de otra manera, una gran desconfianza por parte de los ciudadanos hacia las entidades bancarias y los mecanismos existentes de ingeniería financiera. La gente se empobreció, perdió privilegios sociales, vio peligrar sus ahorros y asistió resignada a rescates y políticas monetarias que se explicaban y aplicaban como imprescindibles.

En un contexto de franca desilusión proliferaron las personas críticas con el modelo existente y las instituciones. La realidad ofrecía un poderoso acicate para la acción de los agentes más extremistas, posicionados en posturas especialmente críticas con el sistema bancario y los gobiernos; un ámbito en el que emergieron perfiles muy libertarios, con talantes ideológicos incluso anarquistas o del tipo ciberpunk.

Ahora pasaremos a hablar de una de esas personas. Aunque en realidad se desconoce la identidad del creador del bitcoin, hay indicios de que bien pudiera haber partido de los entornos citados, que además fueron los primeros que mostraron un especial entusiasmo por el dinero digital. Esto no deja de ser algo lógico teniendo en cuenta la naturaleza independiente respecto a bancos

centrales y gobiernos que ofrece la criptomoneda, y su capacidad de permitir las transacciones de forma descentralizada, lo cual la hace muy atractiva para estos tecnólogos libertarios.

Hoy es evidente que el interés por la criptoeconomía se ha extendido a muchas otras esferas, pero en aquellos momentos de irrupción, sobre todo era esta clase de personas la que estaba detrás de los avances que se estaban produciendo; estas fueron quienes mantuvieron viva la llama de una innovación que todavía era extremadamente minoritaria y desconocida. Y todavía hoy día, habiéndose propagado el universo del dinero digital a todos los ámbitos, siguen constituyendo un sector muy afín a la criptoeconomía. De manera que este era el contexto en el que irrumpió el famoso texto fundacional del bitcoin, y es importante tenerlo en cuenta.

Pero no nos demoremos más y pasemos a descubrir cómo nació el bitcoin y, ya, de una vez por todas, a entender qué es exactamente, sus fundamentos y sus implicaciones.

EL ECONOMISTA VISIONARIO

Como decíamos, en el año de la crisis económica nació el bitcoin, pero casi una década antes ya había habido quien intuyó lo que habría de venir. Me estoy refiriendo al Premio Nobel de Economía, Milton Friedman (1912-2006), uno de los más influyentes economistas del último siglo.

Friedman, radical defensor del liberalismo económico y del mínimo intervencionismo por parte del Estado en la economía, vislumbró en 1999, cuando contaba ya con casi noventa años de edad, el potencial que Internet tendría como uno de los principales agentes para reducir el papel de los gobiernos. Y todavía fue más allá: fue capaz de apuntar la aparición del dinero digital.

Concretamente, lo que dijo Friedman fue:

> Creo que Internet va a ser una de las mayores fuerzas para reducir el rol del gobierno. Sin embargo, lo que todavía falta, pero que pronto se desarrollará, es dinero electrónico fiable, un método por el cual en Internet se puedan transferir fondos de A a B sin A saber nada de B o B de A. De la misma forma que te puedo dar un billete de 20 dólares, entregártelo en mano y que no quede luego registro de dónde vino. Puedes recibir este dinero electrónico sin conocer quién soy yo. Esto pronto se desarrollará en Internet y hará que sea más fácil usarlo. Por supuesto, tiene su parte negativa. A los gánsteres o personas involucradas en transacciones ilegales, también les facilitará llevar a cabo sus negocios.

Es decir, que lo que echaba de menos era el equivalente de lo que hacemos con el dinero en metálico, pero de forma electrónica.

Hoy, para evitar este riesgo de doble gasto, necesitamos una intermediación bancaria o sistemas como el conocido PayPal, o el más actual Apple Pay, y se trata de un proceso que exige cierto tiempo para llevarse a cabo con seguridad —recordemos lo que contaba en la Introducción de las transferencias internacionales—. Y por supuesto, solo se puede hacer sobre el dinero depositado en nuestras cuentas corrientes bancarias y con una cantidad ingente de intermediarios para que se procese la transacción de forma satisfactoria. Sin embargo, lo que anticipaba Friedman, y acertó, era algo que tuviera la misma concepción que tenemos de nuestro dinero en metálico, pero con un manejo electrónico del mismo y de forma nativa y digital.

De manera que el veterano economista ya pronosticó la aparición de un protocolo que faltaba en Internet, esa revolucionaria red descentralizada consistente en una serie de protocolos abiertos de la que ya fue él mismo testigo, que permitía transmitir páginas web —el protocolo http—, correos electrónicos —el protocolo SMTP— o voz —el protocolo VOIP—, pero no valor —todavía —. Era la pieza que faltaba.

Y no fue en lo único en lo que se mostró clarividente, pues de algún modo también llegó a anticipar riesgos como lo que ocurrió con Silk Road —de la que hablaré un poco más adelante—, al alertar sobre el hecho de que las personas involucradas en actividades ilegales contarían con un modo más sencillo de desarrollar sus negocios. De igual forma que el dinero en metálico es la fuente número uno del mundo para usos ilícitos o blanqueo de dinero, su homónimo digital iba a sufrir los mismos problemas, aunque como veremos, las criptomonedas son mucho más difíciles de usar para transacciones ilegales que el dinero en metálico, ya que dejan una traza.

Obviamente, Milton Friedman no llegó a predecir tanto como la tecnología blockchain, pero sí que vio su necesidad, ya que para que fuera posible algo como lo que él vaticinaba, algo que hiciera capaz la transferencia de valor por Internet de forma segura y sin intermediarios y que permitiera operaciones de traspaso de dinero en efectivo, era necesaria una nueva tecnología que sustentara una moneda nativa en Internet.

Y esta gran pieza que faltaba a los protocolos de Internet que demandaba Milton Friedman en 1999, es la que finalmente aportó alguien que se dio a conocer a sí mismo en las redes con el seudónimo de Satoshi Nakamoto.

EL MISTERIO NAKAMOTO

El 31 de octubre de 2008 aparecía en Internet, en el marco de una lista de distribución en la que se hablaba de criptografía, un artículo firmado por un tal Satoshi Nakamoto que habría de revolucionar el mundo. Titulado «Bitcoin: un sistema de dinero en efectivo electrónico de igual a igual» —*Bitcoin: A Peer-to-Peer Electronic Cash System*—, en tan solo nueve páginas, el autor —o autores, ya que se desconoce si son en realidad más de uno, como mucha gente especula — explicaba un sistema de transacciones electrónicas de dinero basado en redes P2P.

Las redes P2P resultarán familiares a la mayoría, puesto que son las que se emplean muchísimas veces para realizar descargas —habitualmente ilegales—, sobre todo de música, series de televisión o películas —la pionera fue Napster, que se centraba en la música, y hoy en día es el modo en que funcionan los populares torrents—. Cuando la gente se descarga algo no lo hace desde un servidor central, sino que todo el contenido está distribuido de forma compartida en la red y así uno va «armando» el fichero al descargarlo. Es por eso por lo que son tan difíciles de censurar o bloquear, porque en realidad no hay un sitio único al que acudir, sino que está todo completamente distribuido. Es decir, aunque se cerrase un ordenador o un servidor —o unos cuantos—, mientras quedaran suficientes conformando la red P2P, el sistema continuaría funcionando. Por eso se dice que son resistentes a la censura.

Pero las redes P2P son mucho más que eso, no ya por la utilidad que la gente les dé en última instancia, sino por su propio concepto, que abre infinidad de posibilidades, pues se trata de redes en la que todos sus miembros se comunican con todos sin que haya nadie que centralice esa comunicación; es decir, no hay intermediarios y son redes completamente descentralizadas. Y esto es lo que habrá de pasar con el bitcoin. No hay una institución central como un banco que intermedie, sino que es una moneda descentralizada, un concepto clave para entender por qué esto es tan revolucionario.

Es por ello que Nakamoto recurrió a este tipo de red para crear su modelo de dinero electrónico, puesto que ya de partida tenía claro que había que evitar la existencia de una institución central que tuviera que encargarse de crear confianza y garantías sobre las transacciones que se realizaran —enseguida pasaré a describir las características y elementos de este sistema de red descentralizada, que ya en ese texto fundacional de Nakamoto quedaba perfectamente definido—. Lo cierto es que el artículo es un poco complicado de

leer porque es muy técnico y es prolífico en conceptos informáticos y criptográficos, pero básicamente debemos entender que ahí estaba la conceptualización de todo lo que iba a ser la tecnología blockchain —aunque en ningún momento se cita todavía este término, que se popularizó más adelante—.

Nakamoto creó, por lo tanto, en 2008 una nueva moneda a la que denominó bitcoin, y a la que presentó como una versión del dinero en metálico, pero vía electrónica, capaz de permitir pagos de forma segura entre dos partes que se mandan de uno a otro sin que haya ninguna institución financiera entre ellos; es decir, de manera, como hemos dicho, descentralizada. Y eso era lo realmente revolucionario. Lo que soñaba Milton Friedman una década antes, Nakamoto acababa de crearlo.

En las transacciones de dinero electrónico actuales donde los bancos intermedian, el rol de ambos bancos —más otros intermediarios en el caso de que los haya— es el de garantizar que el dinero no se gaste dos veces. Es decir, que en el momento que el dinero esté transfiriéndose de mi cuenta a otra, no me lo pueda gastar yo a la vez que la persona que lo recibe. Este problema, que en inglés se conoce como el *double-spend problem* —el problema del doble gasto— es el conflicto fundamental de cualquier sistema de dinero electrónico, y normalmente los sistemas centralizados tradicionales garantizan que esto no ocurra.

Y para garantizar que eso no ocurra es por lo que los sistemas informáticos bancarios son tan cerrados y complicados de integrar o interaccionar con otros sistemas. Sin embargo, Satoshi Nakamoto, con la invención de bitcoin, fue la primera persona en el mundo que consiguió resolver este problema del doble gasto de forma completamente descentralizada y sin la necesidad de la intervención de ningún intermediario centralizado —y eso se consigue mediante lo que se conoce como un algoritmo de consenso entre todos los nodos que veremos más adelante en detalle—.

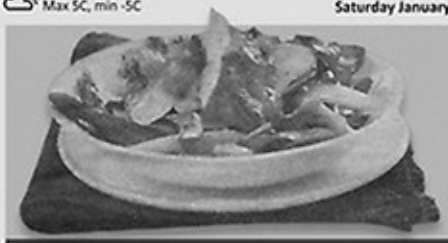
La publicación del artículo fue el pistoletazo de salida. En enero de 2009, Nakamoto distribuyó ya al público la primera versión del software para crear un nodo de bitcoins —enseguida llegaremos a explicar qué son los nodos— en código abierto, con lo que se comenzaron a emitir oficialmente las primeras criptomonedas. A este primer bloque de bitcoins se le llamó Génesis, y contenía concretamente la cantidad de 50 bitcoins que fueron asignados al propio Nakamoto como dueño del primer nodo.

Desde los inicios y hasta hoy, el software de Bitcoin —y de la amplia mayoría de otras criptomonedas y blockchains— ha sido siempre de código abierto,

donde todo el mundo puede descargarlo de forma gratuita y acceder al código fuente del software para ver exactamente qué tareas realiza y cómo.

THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50



Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout Inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it
Body&Soul

Detox in style
The best spas on the planet
Travel

Salmon Rushdie
I Won't Marry Again
Pages 22, 23

Giant Killing?
Guide to the FA Cup Third Round
Sport

Portada del diario *The Times* cuyo titular se ocultaba en el primer bitcoin emitido por Satoshi Nakamoto.

Es muy interesante lo que se descubriría más tarde que venía incluido de manera encriptada en este primer bloque de bitcoins emitido. Es algo que aporta todavía más misterio a lo que rodea a esa enigmática figura de Nakamoto. Con la primera emisión de moneda digital se incluyó un mensaje muy especial: el titular de una reciente portada del diario *The Times* en la que se informaba de un nuevo rescate bancario en el Reino Unido —recordemos que estamos en el contexto de la crisis económica—. La edición de ese día del periódico en cuestión se ha convertido en objeto de culto y ya no se encuentra en el mercado a no ser que sea a precios desorbitados.

¿Por qué quiso incluir este mensaje encriptado el creador de la primera moneda digital? Todo apunta a que se trata de una evidencia más de que la coincidencia temporal entre ambos acontecimientos no es casual, y que el propio Nakamoto pertenecía a esa población, quizás de perfil libertario, especialmente crítica con el sistema financiero y las instituciones. En realidad eso no lo sabemos, pero que existe una relación directa entre el bitcoin y la crisis económica, y que el primero es una respuesta a la segunda, se nos antoja más que evidente.

Y es que acerca de quién se esconde detrás del seudónimo de Nakamoto seguimos, como hemos dicho, sin saber mucho. Tras la emisión del bloque Génesis se siguieron emitiendo más bitcoins de acuerdo con la política monetaria del Bitcoin, que sabemos que, dado que él es uno de los nodos originales, fueron a parar en su totalidad a su monedero, y que nunca después ha transferido ni gastado, por lo que ahora tendrá miles de millones de dólares. Esto se puede comprobar perfectamente, ya que una particularidad del sistema es que todos los registros quedan computados y son accesibles al público, cualquiera los puede ver. Es cierto que son anónimos y solo quedan registradas las direcciones de los usuarios mediante un número. *A priori* no podemos saber quién se esconde detrás de cada uno, pero obviamente conocemos el número atribuible a Nakamoto porque él fue quien realizó la primera emisión y, por lo tanto, es posible rastrear si esa dirección ha utilizado o transferido después sus bitcoins o parte de ellos. Y no lo ha hecho. Sea quien sea, los bitcoins que posee lo convierten en una de las personas más ricas del mundo.

Todo esto forma parte de la leyenda que rodea al universo particular de la primera criptomoneda. Nakamoto se ha encargado de alimentarla. Desde abril de

2011 desapareció casi por completo del mapa. Él mismo escribió a otro desarrollador diciendo que se había «movido a otras cosas», y desde entonces poco se ha vuelto a saber de él. No ha usado sus bitcoins, pero es que, además, ha dejado de participar en foros y debates en la red en los que antes era muy activo, y ya no responde nunca cuando se le alude. Estamos hablando de un experto en criptografía, así que obviamente es alguien capaz de ocultar muy bien sus comunicaciones y movimientos sin dejar ni rastro. Tan solo volvió a dar señales de vida al cabo de un par de años de haber desaparecido, y lo hizo para desdecir una noticia de un periódico que aseguraba que le habían identificado.

La noticia dio mucho que hablar y supuso un foco de atención sobre un falso Nakamoto, de manera que el verdadero hubo de desmentirlo. Volvió a escribir *online* para manifestar que esa persona no era él solo para que lo dejaran en paz. En cualquier caso, esta aparición puntual también permite dejar de especular con que pudiera haber fallecido o tenido algún percance a partir de 2012. Esto hace patente que su desaparición fue, sencillamente, algo voluntario.

De algún modo parece que es como si hubiera cumplido ya con su misión: lanzó la moneda digital, explicó su funcionamiento, aportó el software necesario, creo la comunidad que lo desarrollaría y expandiría, y desapareció. El responsable de uno de los inventos más revolucionarios de los últimos tiempos continúa siendo un completo desconocido y uno de los misterios más fascinantes del mundo de la tecnología.

¿Quién es Satoshi Nakamoto?

Al enorme interés por el bitcoin se une la fascinación por el origen de su creador: un enigmático personaje que se hacía llamar Satoshi Nakamoto. Pero ¿quién es realmente?

Satoshi Nakamoto es un seudónimo detrás del cual se esconden una o varias personas. Parece mentira que todavía no haya podido conocerse tras casi diez años la identidad real de alguien con tantísimo impacto en el mundo. Lo cierto es que quien quiera que fuera o fuese, tenía que ser una persona —o, repito, un grupo de personas— con un altísimo conocimiento en técnicas de matemáticas, criptografía, informática, programación y también economía para poder haber concebido algo tan revolucionario y complejo como el Bitcoin.

Inicialmente, Satoshi Nakamoto se presentó al público como una persona que vivía en Japón y que había nacido en 1975. Sin embargo, su perfecto inglés así como la total ausencia de ningún tipo de palabra o carácter en japonés en sus artículos, e-mails o comentarios en foros, hace pensar que esto no fuera realmente así.

Durante los últimos años y desde que en 2011 desapareciera por completo, ha habido varias teorías e intentos por desenmascarar a la persona que se encuentra detrás de ese nombre. Una de ellas se produjo en 2014, cuando unos periodistas descubrieron a un ingeniero informático llamada Dorian Satoshi Nakamoto viviendo en California, a tan solo unos pocos bloques de Hal Finney, uno de los primeros científicos en colaborar con Nakamoto en el desarrollo de Bitcoin, y el receptor de la primera transacción de bitcoins de la historia.

El descubrimiento de Dorian Satoshi Nakamoto desató una locura mediática, con todos los medios de comunicación intentando conseguir la exclusiva, pero el mismo Dorian rápidamente se encargó de negar que él fuera el creador del bitcoin. En ese momento las sospechas se dirigieron enseguida a Hal Finney, y se especuló con que él fuera Satoshi Nakamoto y simplemente hubiera usado el nombre de su vecino como seudónimo. Finney, además, era también amigo de Nick Szabo, el creador del Bit Gold, que precede al bitcoin, y un reconocido fan de los seudónimos. Desgraciadamente, en 2014 Finney estaba peleando por su vida debido a una enfermedad terminal, la ELA —esclerosis lateral amiotrófica—, que ya no le permitía moverse o hablar, de manera que no pudo nunca confirmar o desmentir este punto.

Por su parte, Nick Szabo, otro candidato a ser Nakamoto debido a su alto conocimiento sobre los temas de monedas digitales y su trabajo pionero en el campo, siempre ha negado ser Satoshi Nakamoto.

Pero hay más candidatos que se barajan. Uno de ellos es el científico y hombre de negocios australiano Craig Wright. De hecho, llegó a ser «proclamado» como Nakamoto por las revistas *Wired* y *Gizmodo* después de una intensa investigación conjunta. Y a diferencia de los otros que siempre lo han negado, Craig llegó a admitir en 2016 que

efectivamente él era Satoshi Nakamoto, e incluso intentó aportar pruebas sobre sí mismo como creador del bitcoin. Esas pruebas consistían en demostrar que tenía acceso a la primera transacción de bitcoin —algo que solo Satoshi Nakamoto podría tener—, pero nunca llegaron a publicarse y los medios de comunicación descartaron que fuera realmente el buscado misterioso personaje, y lo trataron de fraude. Craig Wright continuó un tiempo insistiendo en que era el auténtico Satoshi, y aprovechó la atención hacia su persona para promocionar sus diversos proyectos en el mundo de blockchain.

De manera que así seguimos hoy: el misterio continúa y continuamos sin saber quién es realmente Satoshi Nakamoto, y con serias dudas de que lo lleguemos a saber algún día. Lo que sí está claro es que quien quiera que sea —o quienes quieran que sean—, Satoshi Nakamoto es una de las personas más ricas del mundo, ya que se estima que tiene cerca de un millón de bitcoins, lo cual le llegó a colocar en el puesto cuarenta del mundo por un breve espacio de tiempo cuando en diciembre de 2017 el bitcoin alcanzó los 20 000 dólares de valor. Quizás sea por eso por lo que no quiera que se sepa quién es.

RED MUNDIAL DESCENTRALIZADA

Como explicábamos antes, el artículo de Nakamoto no se limitaba solo a elucubrar con la creación de una criptomoneda digital, sino que, además, aportaba una rigurosa explicación de la tecnología sobre la que se iba a sustentar, así como sobre la política de emisión de bitcoins —es decir, en definitiva diseñaba una política monetaria propia—.

Tras la creación del primer nodo por parte de Nakamoto y la emisión de los 50 bitcoins iniciales en el bloque Génesis, comienza ya a agregarse gente a la red. Una segunda persona, Hal Finney, fue la primera que se descargó el software necesario creado por Nakamoto —el software conocido como Bitcoin Core—, surgiendo de este modo el segundo nodo de bitcoin. Nakamoto envió 10 bitcoins de los 50 primeros a Finney, realizándose la primera transferencia de moneda digital de forma totalmente segura y descentralizada de la historia. Esta transferencia de bitcoins por parte de Nakamoto cabe encuadrarla en el proceso

de lanzamiento y ensayos de la nueva criptomoneda, pues, como ya se ha dicho antes, a partir de ahí se los quedaría él y no movería la práctica totalidad de sus bitcoins.

Poco a poco se fueron añadiendo más personas a la red, descargándose el software y apareciendo así nuevos nodos que son conocidos como mineros, ya que producen bitcoins como un símil a la minería tradicional que extrae metales preciosos como el oro.

Es el momento de explicar más detalladamente qué significan estos conceptos para entender el funcionamiento de esta red descentralizada y la tecnología que hizo posible la existencia del dinero digital. Quiero distinguir los pilares fundamentales sobre los que se sustenta esta red mundial que constituye el bitcoin —y la gran mayoría de las otras criptomonedas y blockchains—: los nodos o mineros, el algoritmo de consenso entre los nodos, los monederos y bolsas virtuales y una política monetaria propia.

En primer lugar, como ya se ha anticipado y sobre lo que se ha insistido porque es esencial, Bitcoin es una red mundial descentralizada de ordenadores que actúan en P2P —todos los componentes de la red se comunican con todos sin que nadie centralice tal comunicación— y cada uno de estos ordenadores constituye un nodo —hoy en día se estima que hay unos 12 000 repartidos por el mundo—, comportándose todos como iguales entre sí, todos conectados con todos.

Como explicábamos más atrás también, es muy importante que fuera una red P2P y descentralizada, pues estando todos los miembros en conexión con todos, no habría nadie en medio que pudiera controlar cómo sucedían las cosas y, además, sería resistente a la censura de la misma por parte de cualquier gobierno o entidad, otra propiedad extremadamente primordial del bitcoin. Asimismo, cualquiera podía convertirse en un nodo, ya que es completamente abierta y el software es de código libre y gratuito. Esta es otra de las grandes ventajas del bitcoin.

Cada nodo cuenta con una especie de libro mayor, un libro de registro de contabilidad en el que se almacenan todas las operaciones que se realizan —y no solo en las que participe ese nodo—; es decir, todo lo que entra y sale del monedero de cualquier participante en la red. En eso se comportan como un banco que lleva la contabilidad, pero aquí el libro mayor no es único, sino que está replicado en cada uno de los nodos existentes. A esto es a lo que se refieren las siglas DLT —*Distributed Ledger Technology*—, libros de contabilidad distribuida, con las que también se conoce a esta tecnología.

Y esto es una ventaja esencial, porque una de las mayores dificultades con las que cuenta el sistema financiero para asegurarse de que las cosas funcionan es garantizar que un mismo dinero no pueda ser empleado dos veces —el citado problema del gasto doble que explicábamos en su momento—. De ahí el motivo por el que tardan tanto tiempo las transferencias internacionales, porque deben establecerse mecanismos de seguridad para que la parte emisora no se pueda gastar el dinero de una transferencia antes de que le llegue a la parte receptora y esta lo pueda gastar a su vez. Ello exige que el sistema financiero se revista de una notoria complejidad para garantizar esta seguridad y confianza.

En el caso del bitcoin, ese libro mayor distribuido consigue que, al estar replicado en todos los nodos, no pueda ser de ninguna forma modificado de manera autónoma: todos los nodos deben estar de acuerdo en cuál es «la verdad», y uno no puede cambiar su verdad sin que lo hagan los otros, evitándose ese problema del doble gasto o la posibilidad de manipular la red y cambiar transacciones pasadas.

Podemos decir que la clave de esta tecnología es el consenso como instrumento para ofrecer confianza: la información es válida y verdadera porque todos los miembros de la red tienen la misma información. Esta propiedad del bitcoin y de las otras criptomonedas es lo que se conoce como la inmutabilidad, la imposibilidad de modificar las transacciones ya ocurridas. De manera que de lo que estamos hablando es de un libro de registro inmutable que contiene la historia completa de todas las transacciones que se han ejecutado en la red; una inmensa base de datos que se distribuye entre todos los participantes.

Es momento de hablar del rol de estos participantes —los mineros— y de la necesaria actividad de minado que desempeñan. Entramos de este modo en el segundo de los pilares básicos a los que hacía mención antes.

Los mineros son el grupo de ordenadores que forman parte de los nodos. El nombre es significativo, pues nos puede remitir a los antiguos buscadores de oro que incansablemente abrían minas y buscaban un filón que les permitiera enriquecerse. En el caso del bitcoin, desempeñan una actividad imprescindible para el correcto funcionamiento del sistema y son incentivados por ello con su «oro digital». Vamos a explicar esto más detenidamente.

Hemos hablado antes de ese libro de contabilidad del que dispone cada nodo y en el que se registran irreversiblemente todas las transacciones que se realizan. El procedimiento es el siguiente: cada vez que se lleva a cabo una nueva transacción, esta se agrega a un bloque. Es decir, que lo que se verifica no es cada transacción, sino los bloques en los que son agregadas. Cada diez minutos

es emitido uno nuevo con las transacciones que se hayan realizado en ese espacio de tiempo. ¿Y cómo se registra en el libro de contabilidad este bloque? Aquí viene una de las partes más interesantes de esta tecnología.

En el momento en que es emitido un bloque, cada nodo compite por descifrar la información que contiene —encriptada sobre complejos problemas matemáticos— y agregarla al libro de contabilidad. Es decir, que si yo realizo una transacción a mi amigo Gonzalo, esta sería lanzada a la red, agregándose a un bloque en el que también se recogerían otras transacciones que se van encadenando unas a otras, y a los diez minutos el bloque es emitido y todos los ordenadores tratan de resolver un problema criptográfico de alta complejidad, puzles criptográficos de una deliberada y enorme dificultad para que la red sea segura. Esto es lo que se conoce como minado.

En cuanto uno de los nodos resuelve el problema, la información es registrada, agregada a la cadena de bloques y todos los demás nodos la replican, quedando fijada ya en el libro de contabilidad de forma inmutable, sin que sea posible modificarla —yo ya no puedo gastarme el dinero que transferí a Gonzalo porque necesitaría modificar el registro no en uno, sino en al menos la mitad de los nodos que hay en la red, algo que quizás sería sencillo con una red pequeña de nodos, pero que aquí resulta prácticamente imposible, puesto que hay, como decíamos, alrededor de 15 000 en todo el mundo—.

Cuanto más grande sea una red y más distribuida esté más segura será. Este proceso es lo que se conoce como algoritmo de consenso, es decir, los diferentes nodos se tienen que poner de acuerdo entre ellos sobre quién valida la transacción y añade el bloque que luego todos los demás también añadirán a su copia del libro mayor.

El meollo para realizar esto de forma descentralizada estriba en que, al no haber una entidad central que decida cuál es el bloque válido que todos añaden, debe hacerse gracias a métodos criptográficos que permitan que se llegue de forma distribuida a este consenso de cómo añadir otro bloque. Esta parte es otra de las grandes contribuciones de la blockchain de Bitcoin.

La idea de la competición por descifrar el problema criptográfico es muy interesante. Y es que, ¿por qué iba la gente a competir por ello cuando exige una fuerte inversión en equipos muy potentes, de alta capacidad de computación y con un consumo energético muy alto? Formulada la pregunta de manera más amplia, ¿por qué se van a molestar en pertenecer a esta red P2P?

Aquí es donde llega la cuestión del incentivo que citamos antes: cada vez que un nodo resuelve el problema y registra el bloque, se emiten nuevos bitcoins que

van al ordenador que ha conseguido agregar ese bloque. El minero ha encontrado el oro.

Que exista un incentivo económico para el minero —y en general, para todo aquel que decida pertenecer a la red y practicar el minado— es muy valioso, puesto que, como sabemos, redes P2P ha habido muchas, por ejemplo, las que hemos mencionado que se emplean para descargar contenidos como la red BitTorrent, que seguro que tienes algún amigo de un amigo que alguna vez ha usado. Pero estas redes tienen un problema, y es precisamente la ausencia de incentivo para que sus miembros sigan formando parte de ella.

No es difícil imaginar que cuando alguien se descarga, por ejemplo, la última temporada de *Juego de tronos*, lo que hace inmediatamente después es cerrar el software que ha empleado para tal fin, puesto que mantenerlo abierto no le aporta nada más que el consumo de sus recursos —menos capacidad de computación y ancho de banda—. Lo cierto es que nadie va a tener interés en pertenecer a la red, y tampoco lo tiene en conservar el fichero descargado en su ordenador —no ganas nada perteneciendo a la red ni manteniendo los ficheros en tu ordenador; al contrario, pierdes recursos de red y computación y almacenamiento—. Ese es el motivo por el que cuanto más antiguo sea el archivo —en nuestro ejemplo, cuanta más vieja sea la temporada de *Juego de tronos*—, más difícil es encontrarlo en la red.

Pero Bitcoin sí que ofrece un incentivo económico para participar en su red: cada vez que se generan bitcoins nuevos, estos se reparten entre quienes forman parte de los nodos. Esto ha permitido que Bitcoin crezca, siga creciendo y que haya cada vez más personas que quieran participar. Por algo tan sencillo como que se gana dinero. La gente invierte por formar parte de ello.

A principios de 2018, el dinero que se había repartido entre los mineros era de unos 4500 millones de euros. No es de sorprender que ahora mismo sea, seguramente, la red de ordenadores conectados más grande que hay en el mundo. Si Bitcoin no fuera una P2P con un buen incentivo económico para pertenecer a ella, no funcionaría. Habría que volver a un sistema centralizado, como un banco, que funciona porque es un negocio en sí mismo, con lo que fracasaría en la premisa primera de su razón de ser.

Y por supuesto es abierto: cualquiera puede formar parte, ya que el software está disponible, como hemos apuntado, para ser descargado por cualquiera. De hecho, al inicio, los primeros mineros lo hacían desde el ordenador de su propia casa. Hoy, la cuestión se ha sofisticado mucho, y si no se dispone de unos equipos de minado con chips especializados y con una capacidad de

computación muy alta, es improbable que te toque a ti poder descifrar un bloque y ganar bitcoins. Lo habitual es que la gente se agrupe en comunidades de varios nodos —lo que se conoce como *pools* o consorcios de minado—, y si alguno le toca, se repartan los bitcoins o fracciones de los mismos.

Uno de los grandes debates de la comunidad de Bitcoin es sobre si es más rentable minar bitcoins —es decir, invertir en máquinas especializadas de minado e incurrir los costes de tenerlas conectadas a la red de Bitcoin veinticuatro horas al día— o simplemente comprarlos. Por mi experiencia personal, minar todavía es una actividad bastante rentable siempre y cuando puedas tener acceso al hardware especializado a un precio razonable y a un coste energético bajo; si no, es mejor comprar bitcoins y esperar a que se revaloricen.

¿Es rentable de verdad el minado?

El proceso de minado normalmente fascina a la comunidad cripto, ya que permite, en cierto modo, «imprimir» criptomonedas. La sensación de abrir tu monedero de cripto por las mañanas y ver que el número de criptomonedas se ha incrementado es algo a lo que es difícil resistirse. Sin embargo, hacerlo de forma rentable no es nada sencillo.

Por un lado, tenemos que conseguir el hardware adecuado y, por otro, debemos tener acceso a electricidad a un precio razonable, ya que las máquinas de minado tienen un elevado consumo energético —una sola equivale a tener un aspirador encendido veinticuatro horas al día—. También necesitaremos algún *data center* donde poner las máquinas, ya que lo de tenerlas en casa no es una opción sensata, pues hay que mantener baja su temperatura —tienden a calentarse mucho—, y eso exige grandes ventiladores instalados, que a su vez son extremadamente ruidosos.

Además, la dificultad de minado suele crecer con el tiempo conforme más máquinas se conecten a una blockchain particular, y a eso hay que sumarle la volatilidad propia de la moneda. Por ello, muchos creen que es más rentable invertir en comprar la moneda que hacerlo en adquirir el hardware y pagar la electricidad. La realidad, como suele ocurrir, está en el punto medio.

Por un lado, si consigues comprar hardware adecuado a un precio razonable, su coste lo puedes recuperar en pocos meses, y a partir de ahí todas las monedas que continúes minando serán básicamente gratis, excepto por el coste de la electricidad. Durante los primeros meses de minado, por lo tanto, no se gana dinero, sino que se intenta recuperar la inversión inicial en hardware.

Si en este tiempo la criptomoneda que estás minando se hubiera apreciado, te habría salido más a cuenta —y proporcionado menos quebraderos de cabeza— haber comprado bitcoins en una *exchange*. Sin embargo, si las criptomonedas no suben de precio o incluso bajan durante un periodo largo, es más rentable minar —y también más gratificante—, ya que una vez pasado la etapa inicial para recuperar la inversión, estarás generando, como hemos visto, monedas prácticamente gratis.

Según mi experiencia, lo más complicado suele ser conseguir el hardware barato, especialmente para monedas como el bitcoin que requieren chips específicos y que se pueden conseguir solamente de unos pocos proveedores, con uno en particular, Bitmain en China, que tiene casi el monopolio en este negocio, con más del 70 % de cuota de mercado.

¡QUE NO TE ROBEN LA CARTERA!

Venimos hablando de la emisión de bitcoins y su asignación a los nodos, pero… ¿cómo se almacenan estos bitcoins? ¿Y cómo pueden adquirirse si uno no forma parte de la red? Llegamos al tercer pilar que establecíamos dentro del edificio del Bitcoin: los monederos —*wallets*— y las bolsas de cambio —*exchanges*— virtuales.

Los bitcoins se almacenan en unos monederos virtuales desde los que cada uno puede enviar y recibir bitcoins. Se trata de una aplicación muy sencilla en la que cuentas con dos claves: una privada —el equivalente a tu password— para acceder al contenido del monedero, y otra pública que te identifica anónimamente, de manera similar a tu dirección de e-mail. Cuando yo le mando

a mi amigo Gonzalo un bitcoin, lo único que necesito saber es su clave pública de la misma forma que para enviarle un mail solo necesito saber su dirección de correo. La red, y sus protocolos abiertos, en ambos casos, es la que se encarga de hacer que la transacción pase. Y viceversa.

Se trata de un concepto poderoso porque permite enviar y recibir dinero de manera sencilla y casi instantánea. Eso sí, si uno olvida su clave privada es como si pierde su cartera en la calle. Se trata del mismo esquema, porque esto no deja de ser dinero efectivo, en metálico, con las mismas ventajas y los mismos inconvenientes. De hecho, se estima que de los 16 millones de bitcoins que se han emitido desde el año 2009 hasta la fecha, alrededor de unos cinco son inaccesibles porque se han perdido las claves privadas de los monederos que los contienen.

Hay que aclarar también que no es que tu bitcoin —u otra moneda— esté en tu monedero: la moneda en sí está en la red de Bitcoin y su existencia desde el día de emisión, así como todas sus transacciones están replicadas en el libro mayor del que cada ordenador tiene una copia. El monedero lo que tiene es la clave privada que te permite visualizar el contenido de la blockchain y transaccionar con tus monedas. En realidad, se deberían llamar más bien llaveros que monederos, aunque el símil con este último funciona mejor.

El propio software de Bitcoin que se necesita para ser un nodo de la red y minar bitcoins —el Bitcoin Core—, contiene un monedero, ya que es necesario para recibir los bitcoins que te puedan llegar a tocar si verificas un nodo. Sin embargo, para la mayoría de los usuarios, descargar e instalar el software completo de Bitcoin Core es completamente impráctico y complejo, así que hay muchísimas alternativas para usar monederos tanto en el ordenador personal como en los dispositivos móviles. Los más populares son Electrum, Jaxx, Rippex o Exodus y muchos de estos soportan múltiples criptomonedas y no solo bitcoins.

Por otro lado, para comprar y vender bitcoins existen las *exchanges*, las bolsas de cambio de bitcoins. Aquí cualquiera puede cambiar el dinero tradicional de la divisa que sea y comprar bitcoins según la cotización del momento, que estará fijada de acuerdo con la ley de la oferta y la demanda. De esta manera, tus euros pasarán a ser bitcoins y se quedarán atesorados en tu monedero virtual según el protocolo de la blockchain de Bitcoin, ese protocolo que nos faltaba, el que echaba de menos Friedman, el que nos permite ya transferir dinero o valor.

Las *exchanges* tienen monederos donde se almacenan las criptomonedas que un usuario está comprando y vendiendo, pero esos son los que se conocen como

monederos centralizados, ya que el usuario final no tiene acceso a la clave privada de su monedero, sino que esta está gestionada por las *exchanges*, de manera que no se recomienda usarlas para guardar monedas, solo para comerciar con ellas.

La *exchange* más popular y por la que mucha gente empieza en el mundo de las criptomonedas es la americana Coinbase, que opera desde el año 2013. Se estima que tiene ya más de diez millones de usuarios y cerca de 35 millones de *wallets*, y sigue creciendo fuertemente. La razón por la que la gente usa Coinbase es por su sencillo interfaz y soporte, tanto en web como en móvil. Sin embargo, Coinbase tiene pocas criptomonedas y unos costes de transacción altos, por lo que los usuarios más avanzados recurren a otras opciones.

La siguiente opción sería, por lo tanto, una *exchange* como Bittrex, donde se pueden comprar y vender hasta cerca de doscientas criptomonedas diferentes. Otras alternativas son *exchanges* como Bitfinex, CEX.IO —europea— o la más reciente y altamente popular *exchange* china Binance. Hoy por hoy, para usar una *exchange* y comprar cualquier criptomoneda es estrictamente necesario pasar por un proceso de aprobación y de verificación de identidad y de país de residencia para asegurarse que se está comprando de forma legal. Por eso, entre lo que se demoran estos trámites y lo que se tarda luego en enviar fondos desde un banco para empezar a comprar criptomonedas, el proceso puede llevar más de una semana.

Los conceptos de monedero y bolsa de cambio descritos son extensibles al resto de criptomonedas.

Los monederos físicos: la alternativa más segura para guardar tus criptomonedas

Tal y como hemos explicado, las criptomonedas son como el dinero en metálico, y si pierdes la clave privada de tu monedero es como si perdieras un monedero con un montón de billetes y monedas. Y no solo estás expuesto a perderlas, también puede ser que si dejas copias de las mismas en tu ordenador te expongas a que un *hacker* consiga entrar y te las copie o se te instale algún tipo de *malware* que acceda a ellas y las envíe fuera, y una vez se ha hecho con ellas, mueva tus criptomonedas a su monedero.

Por otro lado, si dejas el dinero en las bolsas de cambio o *exchanges* estás sujeto a depender de sus medidas de seguridad, y como venimos diciendo, todavía falta madurez dentro de este mercado y se sufren muchos ciberataques, por lo que las *exchanges* son hackeadas con demasiada frecuencia, robándose criptomonedas y pudiendo perder tu inversión.

Así que lo preferible es controlar tu propio destino. Para ello, la mejor solución son los monederos físicos. Estos son unos dispositivos que tienen una capa de seguridad más allá de la que ofrecen los monederos software, o la opción de imprimir la clave privada y guardarla en una caja fuerte —esto es lo que se conoce como monederos en papel—.

Estos dispositivos físicos cuentan con un chip seguro que hace que no podamos usarlos sin autentificarnos con nuestra clave privada. Pero la parte más interesante es que si se rompen o los perdemos, es posible restaurarlos —y recuperar el acceso a las criptomonedas— con una combinación de palabras o semilla de recuperación que se incluye con ellos cuando los compramos.

Estos monederos, a pesar de su precio que puede llegar a rondar los 50 o 100 euros, dependiendo del modelo, es la forma más segura de almacenar criptodivisas. Cualquier persona con una inversión importante en criptomonedas debería plantearse seriamente comprar uno de estos monederos hardware.

¿UNA MONEDA «DE VERDAD»?

Nos queda explicar el último de los pilares fundamentales del bitcoin: su particular política monetaria. Pero, claro, si hablamos de política monetaria surge una pregunta de partida que, además, seguramente oigamos a nuestro alrededor constantemente: ¿es el bitcoin una moneda de verdad?

El bitcoin es la primera de las criptomonedas. La parte de «cripto» es bastante evidente: a este dinero se le antepone el prefijo *cripto-* porque se trata de monedas digitales que dependen de técnicas de criptografía para asegurarse que

las transferencias que se realizan con ellas son seguras. La criptografía —del griego *criptos* u ‘oculto’, y *grafé* o ‘escritura’, es decir, escritura oculta— es el ámbito de la ciencia y la tecnología que se encarga de desarrollar las técnicas de cifrado o codificación que permiten hacer los mensajes ininteligibles o encriptados para que solo puedan ser leídos por los destinatarios adecuados.

Uno de los pilares de la criptografía es lo que se conoce como funciones resumen —en inglés, funciones *hash*—. Estas son conocidas como funciones unidireccionales, y son muy fáciles de computar en una dirección, pero difíciles de hacerlo en dirección contraria. Un ejemplo muy básico: si le formulas a alguien 4 + 5, inmediatamente te responderá 9; no obstante, si lo que propones es que tienes un 9 y le pides al otro que te diga cómo se ha obtenido, no tiene otra opción que probar las distintas posibilidades (1 + 8, 2 + 7, 3 + 6, 4 + 5…). Esa es la base de la criptografía.

Los algoritmos criptográficos permiten que la red sea segura y que un ordenador no pueda revertir matemáticamente una operación. La criptografía es una ciencia que existe desde el siglo V a. C., y que ha ido evolucionando a lo largo de la historia hasta llegar a la informatización, siendo la época de Internet cuando más se ha utilizado para encriptar cosas como páginas web o correos electrónicos.

En las criptomonedas, en general, y en el bitcoin, en particular, la criptografía se usa para resolver el llamado dilema de los generales bizantinos. Este problema trata de buscar una solución técnica que permita alcanzar un acuerdo entre varias partes —los generales bizantinos— que no confían entre sí y de forma descentralizada; es decir, sin necesidad de acudir a una autoridad central. La resolución práctica de ese dilema por primera vez en la historia es lo que resuelve el algoritmo de consenso de Bitcoin y lo que ha dado lugar a la tecnología de blockchain. Es decir, lo que los mineros de Bitcoin hacen es computar una función de *hash* en la única dirección que pueden hasta que uno de ellos encuentre cuál era la entrada correcta y ese mismo es el que valida el bloque y recibe como premio los nuevos bitcoins que se están emitiendo.

De modo que la parte *cripto* queda clara, pero la de «moneda» ofrece más controversia. Recordemos las tres funciones que debía cumplir una moneda y que presentábamos en el primer capítulo en la breve historia del dinero: una moneda es algo donde puedes almacenar valor, algo que puedes intercambiar y que te permite pagar y hacer transacciones; y algo que sirve como referencia de valor, con lo que puedes referenciar el precio de las cosas.

La gran pregunta es: ¿cumple el bitcoin estas tres condiciones? Lo cierto es que hoy por hoy ni el bitcoin ni prácticamente ninguna de las criptomonedas las cumplen. La característica que más se satisface es la de almacenamiento de valor: sirve para guardar dinero y, además, tiene la ventaja de que no se devalúa —como una especie de oro digital, pero siendo muy portable, no como el oro—. Sin embargo, las otras dos condiciones aún no se cumplen.

Aunque poco a poco se va extendiendo como medio de intercambio, todavía el bitcoin no es aceptado en muchos sitios, puesto que está en una fase emergente y sufre problemas de escalabilidad para soportar millones de transacciones por segundo y sin incurrir en un alto coste. Y como medida de unidad de valor, hay que reconocer que tampoco resulta muy válido, puesto que aún tiene muchísima volatilidad y sus cambios de valor son muy altos y muy acelerados en el tiempo y, por lo tanto, es difícil usarlo para referenciar el valor de un objeto.

De manera que hay que reconocer que el bitcoin no cumple plenamente todavía todos los rasgos que cabría exigir a una moneda estable. Sin embargo, a pesar de ello, cuenta, eso sí, con una política monetaria perfectamente definida desde el principio, desde la propia formulación teórica de la moneda, y antes incluso de la primera emisión de bitcoins. No cabe duda de que la visión de Nakamoto era a futuro, y anticipando y confiando en su establecimiento como «moneda completa».

Y es que en el famoso artículo de 2008 también se explica una política de emisión de bitcoins, que en absoluto es arbitraria, sino que sigue, no las directrices de un banco central, sino un algoritmo perfectamente establecido. Aquí todo es digital.

Porque ya sabemos que las políticas monetarias están controladas por los bancos centrales de los países, que son los que tienen potestad para emitir más o menos en función de las necesidades o utilizar otras palancas para controlar la cantidad de dinero líquido disponible en el mercado, tales como la compra o la emisión de deuda y bonos del Estado, o la tasa de interés. Sin embargo, en el caso de una moneda digital descentralizada no tenemos, por definición, ninguna autoridad central. En cambio, se cuenta con un algoritmo definido desde el principio; uno que incorporan todos los nodos y que no es modificable. Y este algoritmo determina de manera fija y de antemano, a diferencia de las políticas monetarias de los bancos centrales, exactamente los bitcoins que se emiten en cada momento: cuántos y a qué ritmo.

Lo primero es entender que el número de bitcoins que se emitirán en total es un número finito y prefijado, concretamente 21 millones. La fórmula concreta consiste en empezar emitiendo 50 bitcoins cada diez minutos —es decir, cada vez que se añade un bloque nuevo con transacciones a la blockchain de Bitcoin —, y cada cuatro años la cifra se divide por dos. Es decir, desde 2009 se emitían 50 bitcoins cada diez minutos, en el cuatrienio siguiente 25, a día de publicación de este libro, año 2018, se están emitiendo 12,5 bitcoins cada diez minutos, y esta cifra se reducirá a la mitad en 2020.

Hay que recordar que estos bitcoins que se emiten los recibe el minero que haya encontrado la función de *hash* que explicamos antes. Es decir, hoy por hoy, de las decenas de miles de mineros que hay operando en la red de Bitcoin, el que valida el bloque para añadir a la blockchain de Bitcoin con una serie de transacciones es el que se lleva los 12,5 bitcoins —lo cual, a principios de 2018, significa aproximadamente unos 120 000 dólares—. Como también hemos explicado, si el minero está en un *pool* o minando de forma agregada con otros, esos 12,5 bitcoins se repartirán entre todos, con lo cual a cada uno le tocará un poco.

De acuerdo con esta progresión, llegará un momento en que se dejarán de emitir bitcoins, y mucho tiempo antes la emisión será muy pequeña. Tal es así que entre 2009 y 2017 se emitieron ya aproximadamente 16,5 millones de bitcoins, y aunque no será hasta el año 2140 que se terminen de emitir todos, esto significa ya más de las tres cuartas partes de los 21 millones totales que se habrán emitido.

De manera que, mientras los bancos centrales cambian permanentemente su política monetaria, aquí nos encontramos con un algoritmo rígido e inmutable. Esto significa que lo que puede devaluarse en realidad no es el bitcoin, sino las divisas tradicionales como el euro. Podemos decir que los bitcoins tienen cada vez más valor, porque no se puede alterar su cantidad de emisión; cada vez se emiten menos, pero cada vez hay más demanda, ofreciendo así mucha más capacidad de almacenar valor que cualquier otra moneda.

Y es que lo más interesante de esta política monetaria es que asume el concepto de fondo del patrón oro, y el valor de que el dinero sea escaso. Esto es importante: la política monetaria del bitcoin introduce la idea de escasez y deflación en su propio protocolo. Por eso, si se extiende el uso de bitcoins como medio de pago, al ser cada vez más escaso y difícil de conseguir, está cumpliendo una función esencial del dinero. Eso sí, el bitcoin es una moneda que puede fraccionarse hasta ocho dígitos, es decir, cada uno puede dividirse

hasta en 100 millones de fracciones. Una cien millonésima parte de un bitcoin es lo que se conoce como un satoshi (0,00000001 B|).

Para intensificar todavía más la idea de escasez, hay que tener en cuenta que de esos casi 17 millones emitidos, como habíamos comentado antes al explicar el concepto del monedero, 5 millones se consideran ya inaccesibles. Al principio el bitcoin no valía nada, y la gente olvidaba las claves privadas de sus monederos, o se quedaban almacenados en ordenadores viejos que se rompían y eran tirados a la basura.

Por esta idea de escasez decíamos que, como el oro, el bitcoin es muy valioso como almacenamiento de valor, porque no puede ser devaluado, es decir, no puede intervenir un banco central y de forma arbitraria empezar a emitir bitcoins nuevos como ha pasado con el euro en Europa durante la época de la crisis. Podrá subir o bajar su cotización dependiendo de su demanda, pero no devaluarse.

Hay un elemento también importante. El bitcoin es también la primera moneda resistente a la censura. Su política monetaria inmutable y determinista, y su funcionamiento a través de redes P2P descentralizadas hacen imposible, como hemos dicho, que ningún gobierno pueda intervenirlo ni censurarlo. No se puede cerrar la red, ni alterar la política monetaria, ni llevarse los bitcoins. Por eso también es atractivo para sus usuarios, y esos perfiles libertarios y antisistema que ya citábamos antes se mostraron tan afines a este modelo de dinero digital. Y por eso, el bitcoin tiende a ser más adoptado en países totalitarios, donde hay una alta desconfianza hacia el gobierno.

Es buen momento para recuperar la breve historia del dinero con la que arrancábamos esta primera parte, y recordar el patrón oro y la concepción inicial del dinero que en los últimos tiempos se venía distorsionando. Por eso el encabezamiento de esta primera parte cobra mayor sentido. Por eso hablamos con mayor propiedad si cabe de oro digital.

3
EL DINERO DIGITAL HA LLEGADO PARA QUEDARSE

MONEDA EN PROCESO

El bitcoin nació con su política monetaria perfectamente diseñada, y, sin embargo, hoy por hoy, todavía no podemos concederle el cumplimiento de los tres requisitos exigibles a una moneda. No nos conviene olvidar que, por muy acelerados que sean los tiempos, la primera emisión de bitcoins fue en 2009, y evidentemente, la consolidación del dinero digital se encuentra todavía en proceso, en evolución.

Hay quienes hablan de que la historia del bitcoin se escribe en tres etapas distintas: una primera que se correspondería al periodo que va entre 2009 y aproximadamente 2014, que vendría a ser la era inicial del «libre ofrecimiento de Nakamoto»; una segunda, que es en la que estaríamos ahora, que sería la del «subsidio de Nakamoto»; y una tercera, que está por llegar, que sería ya la de la autosuficiencia. Puede debatirse esta cronología sobre la base de distintos hitos experimentados en su evolución, pero sí resulta razonable considerar el ciclo de la moneda de acuerdo con ciertos periodos más o menos diferenciados y teniendo en cuenta que su tiempo de madurez está todavía por llegar.

Es importante, por lo tanto, que, además de conocer los elementos que definen el bitcoin que explicábamos en el capítulo anterior, observemos también la evolución histórica que ha experimentado en estos pocos años de existencia, en los que ya ha habido unos cuantos acontecimientos significativos. Todo ello nos ayudará a comprender mejor el futuro de la criptoeconomía y de todo lo que implica.

El arranque en aquel 2008 de la crisis económica mundial con un famoso artículo publicado en Internet ya lo conocemos, aunque podríamos hablar también de unos años prebitcoin que se remontarían hasta 1998, y en los que se produjeron otros intentos de crear criptomonedas digitales, como el B-money o

el Bit Gold, que fueron formuladas y desarrolladas, pero nunca consiguieron consolidarse y acabaron desapareciendo, aunque introdujeron ya conceptos que luego aparecerían en el bitcoin como el uso de las funciones de *hash* para el consenso de la red mediante lo que se conoce como *proof-of-work* o prueba de trabajo, o el concepto de monedas digitales con una política monetaria que fomenta la escasez. Precisamente, detrás de las mismas se encontraban personas como el ciberpunk Wei Dai —creador del B-money— o el reconocido criptógrafo Nick Szabo —que estaba detrás del Bit Gold, y de quien se rumorea mucho, como ya hemos comentado, que podría ser el auténtico Nakamoto— que fueron de los primeros en pasar a formar parte de la red Bitcoin.

El primero que oficialmente se unió a la red, ya lo sabemos, fue Hal Finney, quien ya en enero de 2009 se descargó el software creado por Nakamoto, dando lugar a un segundo nodo y a las primeras emisiones y transacciones de bitcoins. Otra personalidad importante en el proceso fue Gavin Andresen, que terminó heredando el liderazgo en la comunidad de desarrolladores de Bitcoin una vez que Nakamoto decidió desaparecer de la faz de la tierra. Andresen creó la Bitcoin Foundation, que es la institución responsable de este software abierto, con una gobernanza descentralizada, como no podía ser de otra manera.

Durante aquel primer año se fueron agregando más nodos y se fue ampliando la red, y aparecieron evidentemente los primeros mineros, pero todavía la actividad se limitaba a un minado de bitcoins sin ningún valor, puesto que no se podían comprar ni utilizar para intercambiar productos, y nadie les había fijado un precio. Fue en octubre de 2009 cuando uno de los miembros de la comunidad, que se hacía llamar New Liberty Standard, proclamó la necesidad de contar con un lugar en el que poder comprar los bitcoins con divisas reales. Él mismo realizó el primer intercambio en este sentido, comprando a otro miembro de la red 5050 bitcoins por 5,02 dólares que le pagó por PayPal. Es decir, que cada dólar le proporcionó más de 1000 bitcoins.

Pero no sería hasta el año siguiente, 2010, cuando se creó la primera *exchange* pública que permitió adquirir unidades de bitcoin a personas fuera de la red de nodos a un cambio determinado con respecto a una divisa tradicional. Con la creación de una bolsa de cambio, el bitcoin pasaba a tener un precio oficial por primera vez.

En aquel momento, los primeros tipos de cambios públicos se realizaron a 1 bitcoin por 0,003 dólares. Algo insignificante, cierto, pero para el año siguiente, en 2011, el bitcoin ya había alcanzado la paridad con el dólar, lo cual es considerado otro de los hitos significativos en su evolución. En 2017, esos 0,003

dólares iniciales a que cotizó por primera vez el bitcoin llegaban a ser 20 000 dólares.

EL VALOR DE UNA *PIZZA*

Obviamente, el periplo seguido por un bitcoin que empezó valiendo ni siquiera un centavo de dólar y llegó a valer decenas de miles, es no solo acelerado, sino apasionante y jalonado de hitos y puntos de inflexión. Pero volvamos a aquellos primeros momentos en que el bitcoin comienza a adquirir un valor real.

En mayo de ese mismo año 2010 que el bitcoin cotizó por primera vez en una bolsa de intercambio digital pública, y de este modo contó por primera vez con un valor traducible a nuestras divisas tradicionales, se produjo también el primer pago en bitcoins por un producto.

El programador informático estadounidense Laszlo Hanyecz tuvo el honor de ser el primer usuario en utilizar sus bitcoins para comprar un bien tangible, en su caso un par de *pizzas* de la conocida cadena Domino's Pizza —aunque sobre esto hay confusión, pues luego hay fotos en las que se le ve con unidades de *pizza* de otra marca: Papa John's—. El caso es que, en realidad, la cadena —fuera la que fuera— no aceptaba, como ningún otro comercio o empresa en aquel momento, pagos en bitcoins, de manera que Hanyecz pagó 10 000 bitcoins —que equivalían a 25 dólares en ese momento— a un joven británico de dieciocho años, Jeremy Sturdivant, quien sí aceptaba el dinero digital y que fue quien efectivamente realizó el pedido.

Es decir, que en esos momentos, para poder realizar una transacción con bienes reales la única forma era la que Hanyecz utilizó: pedir a otra persona —que sí aceptara los bitcoins— que hiciera de intermediario para realizarle su compra. Sin embargo, por ello no deja de ser la primera transacción que tradujo dinero digital en un bien tangible, y en su honor se conmemora el Bitcoin Pizza Day, todo un hito en la historia de la criptoeconomía.

Es evidente que entonces no se le concedía especial valor al dinero digital, pero lo cierto es que esos 10 000 bitcoins han llegado a ser 180 millones de dólares en algún momento, lo cual no está mal como precio de dos *pizzas*. Aún hoy se sigue bromeando con el asunto, y hay incluso una cuenta de Twitter que cada día publica cuánto cuestan las *pizzas* que Hanyecz compró. En el momento

en que escribo estas páginas, la ya famosa Bitcoin Pizza vale más de 100 millones de dólares.

Estos primeros años ponen en evidencia que ese periodo no fue sino una especie de campo de pruebas, quizás poco más que un juego para muchos. Recordemos que sus participantes venían a ser en buena medida ciberpunks, anarquistas digitales, personas antisistema, o si se quiere el término popular inglés, unos *geeks*. Sin embargo, estos *geeks* estaban creando algo revolucionario, y a partir más o menos del año 2011, cuando ya se habían producido algunos hitos como la aparición de *exchanges,* la compra de bienes tangibles como unas *pizzas*, o la paridad con el dólar, las cosas comenzarían a cambiar, y lo que parecía un coto de gente antisistema se abrió ya a círculos más amplios, comenzando a participar de la red perfiles muy diversos.

El bitcoin empezaba a hacerse popular, e incluso la revista *Forbes* le dedicó un artículo. Eso provocó que su precio empezara a dispararse, y en mayo de 2011 valía ya nueve dólares. Poco después de haber alcanzado la paridad, su valor se multiplicó por nueve. Enseguida, en octubre de 2011, otra revista muy popular y considerada seria, *The New Yorker*, también le dedicó un artículo «The Crypto-Currency», y el precio volvió a dispararse triplicándose inmediatamente. De este modo, el valor de los bitcoins emitidos hasta ese momento superaba ya los 100 millones de dólares, y comenzaba a ser una cuestión digna de llamar la atención.

No es de extrañar, por lo tanto, que desde Silicon Valley también giraran los ojos hacia el bitcoin, porque empezaron a apreciar que ahí residía un posible cambio en una tecnología con muchísimo potencial. Fred Wilson, un inversor muy reconocido en el terreno del capital riesgo, habló con gran entusiasmo de ello y lo vio como algo realmente transformador.

La criptoeconomía comienza, por lo tanto, a convertirse en una realidad: las altas esferas tecnológicas y financieras le prestan ya atención, empiezan a ser posible las compraventas con bitcoins, Wikipedia acepta la moneda en las donaciones que recibe, nacen otras criptomonedas —como enseguida veremos— … El proceso parecía imparable a partir de 2011. Pero todavía habría que superar alguna que otra prueba.

EN LAS PROFUNDIDADES DE INTERNET

En el dinámico contexto que acabamos de describir, irrumpe una página web un tanto particular llamada Silk Road. Esta se alojaba en la *Deep Web*, la web profunda —u oculta, o invisible, de todas esas maneras se la conoce—, a la que solo se puede llegar mediante un software específico que permite acceder a direcciones de IP encriptadas. Con nuestras conexiones cotidianas y a través de nuestros navegadores y buscadores habituales ninguno de nosotros puede acceder a esas páginas.

Pues bien, en la Internet profunda, Silk Road, creada en 2011, empezó a hacerse muy popular, puesto que a través de ella se podían comprar todo tipo de cosas o servicios, predominantemente de carácter ilegal. Al principio se trataba de drogas, pero pronto el negocio incorporó prostitución, armas e incluso asesinos a sueldo. Todo un mercado negro digital.

En ese momento de auge del bitcoin, desde esta web se pensó que aceptar los pagos con la criptodivisa sería buena idea, puesto que entonces podía ser una excelente manera de garantizar el anonimato de los participantes en los negocios ilegales —y de hecho, en ese momento en efecto se podían comprar bitcoins de forma anónima, aunque eso hoy es casi imposible, puesto que la mayoría de las *exchanges* exigen, como hemos dicho, un registro y una identificación—.

Es así como los bitcoins se convierten en el método de pago estándar en esta web, y eso hizo también que subiera su cotización, puesto que la criptomoneda acababa de encontrar un potente «caso de uso». Resulta triste admitirlo, pero lo cierto es que el primer verdadero caso de uso del bitcoin fue para realizar compras ilegales. Tampoco es de sorprender, puesto que al fin y al cabo, como sucede en el caso del dinero fiduciario, la mejor manera de pagar negocios fraudulentos es mediante el dinero en metálico, y las criptomonedas no dejan de ser su equivalente en la red.

Algo así no tardó en llamar la atención de las autoridades, y en octubre de 2013 el FBI cerró la web y se detuvo en San Francisco a la persona que estaba detrás de ella, Ross Ulbricht. La consecuencia para el bitcoin fue inmediata, produciéndose el desplome de su precio, pues en esos momentos mucha gente lo había atesorado para emplearlo en las compras que se ofrecían desde Silk Road, y acababa de dejar de serles útil. El bitcoin había perdido su principal aplicabilidad y, además, se había creado una pésima reputación por aparecer vinculado a este tipo de negocios.

Esta imagen negativa como moneda utilizada para las transacciones ilegales le ha perseguido durante su historia y hoy todavía me encuentro con gente que me dice que nunca comprarán con bitcoins porque se puede usar para compras

ilegales. A lo que yo suelo responder que me parece perfecto, y que me den todo el metálico que llevan encima, ya que el medio de pago más extendido para las transacciones ilegales sigue siendo, muy por encima de cualquier otro, el dinero en metálico.

En esos mismos años, Bitcoin sufrió, además, otro contratiempo que le dañaría considerablemente también la imagen. En esta ocasión el conflicto tenía mucho que ver con la seguridad del ecosistema creado y los riesgos de *hackeo*.

Desde 2011, la *exchange* MtGox, afincada en Japón, era la bolsa de intercambio de referencia, la que más usaba la gente para comprar bitcoins. Sin embargo, en 2013 empezaron a circular rumores de que muchos de los bitcoins que tenía la gente depositados en esta bolsa se habían perdido. Ya en 2014 se decidió parar todas las transacciones porque se hacía necesaria una revisión. Finalmente, los responsables de MtGox confirmaron que se habían perdido nada menos que 750 000 bitcoins, que se habían ido robando poco a poco durante años sin que ellos fueran conscientes y se declararon en bancarrota.

En agosto de 2015, el CEO de MtGox, el francés Mark Karpelès, fue arrestado por la policía japonesa porque se sospechaba que él mismo había estado desviando bitcoins para su beneficio. En el juicio celebrado en julio de 2017, Karpelès se declaró no culpable. Y en el momento de la publicación de este libro se encontraba en Japón con libertad bajo fianza sin poder salir del país, pendiente de su juicio.

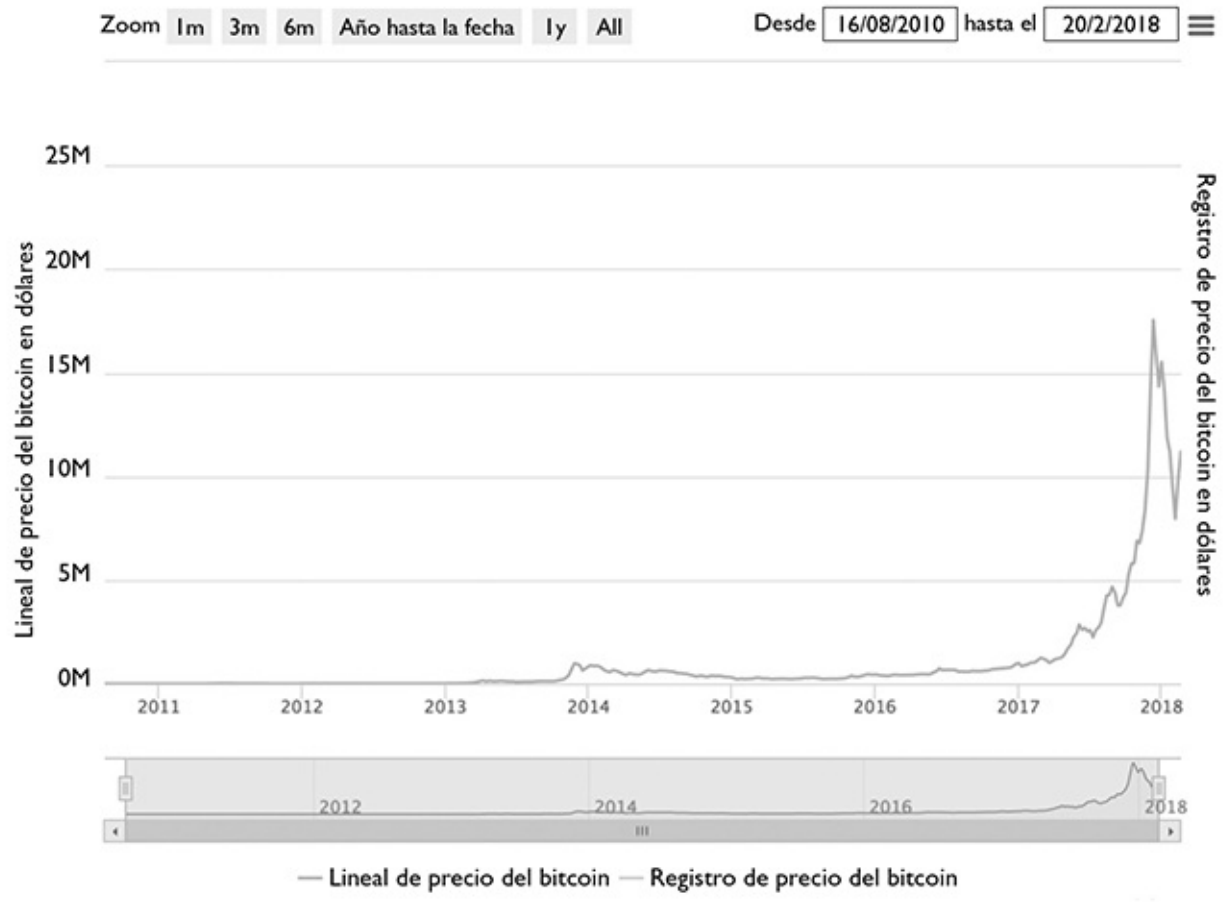
Como era de esperar, aquello provocó que de nuevo se produjese una gran caída —de un 36 % en unos pocos días— en el valor de los bitcoins y la sensación de que había una serie de problemas de seguridad que, aunque realmente no justificados, como veremos en la última parte de este libro, habrían de resultar determinantes en la evolución de la criptomoneda pionera.

UNA BOLA DE NIEVE EN CRECIMIENTO

Es un buen momento para recapitular y hacer balance de la evolución que experimentó el bitcoin en todos aquellos primeros años.

Hemos de distinguir una primera etapa desde su creación en 2009 hasta aproximadamente el año 2011, en que su valor es casi nulo o muy bajo, pero determinados hitos como la aparición de las primeras *exchanges*, su empleo para realizar compras de bienes tangibles, su paridad con el dólar, su aceptación por parte de entidades tan importantes como Wikipedia y WordPress, y el

incremento de su popularidad entre expertos tecnológicos y financieros, le llevan a incrementar el valor hasta alcanzar los 1000 dólares en 2013.



Evolución del bitcoin desde 2011 hasta 2018.

Sin embargo, justo en este momento se suceden los escándalos de Silk Road y MtGox y su valor vuelve a derrumbarse. El periodo siguiente, el que va desde 2014 hasta principios de 2017, podría ser visto como una dura travesía por el desierto, aunque en ese momento vuelven a ocurrir sucesos muy significativos que le llevarían a principios de 2017 a volver a alcanzar aquellos 1000 dólares de 2013.

En el gráfico anterior se puede observar que una vez que el bitcoin alcanzó los 1000 dólares a principio de 2017, se produjo un crecimiento exponencial nunca antes experimentado, y llegó a cotizar incluso a 20 000 dólares, aunque luego se derrumbó hasta cerca de los 7000 dólares —cuando escribo esto, cotiza de nuevo por encima de los 10 000 dólares. Inevitablemente, cuando leas estas páginas, la

información sobre el precio del bitcoin estará completamente desactualizada y es difícil de predecir por dónde andará—.

¿Qué ocurrió en 2017 que ha sido considerado el año Netscape del bitcoin, el año en que de verdad se populariza y está en boca de todo el mundo e incluso sale a bolsa?

Seguramente, algunos hechos ya acaecidos empezaron a influir, como que el Bitcoin fuera declarado en 2015 un *commodity* —un producto básico como las materias primas o el oro— y empezara a ser legislado, lo cual facilitaría la legalización en 2017 de los derivados financieros del Bitcoin, que por primera vez aparecen a últimos de 2017 y fueron los culpables de la fuerte subida de final de año.

También influyeron seguramente aspectos de la política internacional ocurridos a finales de 2016, como el Brexit británico o la elección de Donald Trump como presidente de Estados Unidos, que volvieron a incrementar la negatividad de la gente con respecto a la política y las instituciones, en cierto paralelismo a lo que se sentía en 2008.

Hay que tener en cuenta que hasta ese 2017 en realidad solo los más informados y entusiastas de esa tecnología y de la criptoeconomía tenían bitcoins y hacían algún uso de ellos, pero justo en el verano de ese año, y fomentado por las redes sociales, se produce un *boom* popular e informativo acerca de la criptomoneda.

Ya sabemos que vivimos en una sociedad en la que la información circula a toda velocidad y se propaga a todas partes a través de Internet. Y cuando algo provoca tanta atención y empieza a ser adoptado por muchas personas, muchas más se van incorporando, produciéndose un efecto de bola de nieve. En este caso participó mucha gente que no sabía, casi seguro, dónde se metía. Y hubo un pico muy llamativo en diciembre de 2017, coincidiendo con fechas señaladas donde muchas familias se reúnen —el día de Acción de Gracias en Estados Unidos, o posteriormente la Navidad y el Fin de Año en la mayoría del mundo—. Se especula que en bastantes de estas reuniones el tema de conversación fue el bitcoin y, como había subido espectacularmente, provocó que más gente lo quisiera utilizar como inversión.

Habrá que admitir que se trató de una subida en ese momento demasiado injustificada, excesiva, pero que daba fe de un fenómeno que tenía un potencial enorme y que estaba madurando mucho.

Es en ese momento también cuando se legalizan en Estados Unidos y Canadá los productos derivados del Bitcoin. Se trataba de productos financieros

indexados como ya existen para otros casos —oro, divisas, *commodities*…—. Es común en el mercado financiero de lo que el Bitcoin también ha terminado participando desde que a finales de 2017 se aprobaron las licencias y se hizo legal en las *exchanges* de futuros y derivados más importantes de Estados Unidos.

Todo eso también influyó en la valoración del bitcoin y en su mercado, porque estos derivados ofrecen mayor confianza a muchos especuladores, ya que permiten apostar tanto a favor como en contra de su valor, reforzando las variaciones un tanto artificiales en el valor del bitcoin. Es algo que ya pasó de forma similar cuando salieron los primeros derivados del oro, que también terminaron provocando la caída de su valor para a la larga convertirlo en algo más valioso que antes de que irrumpieran en el mercado.

Es de prever que con el bitcoin esté ocurriendo lo mismo, aunque hoy en día todo se comprime en el tiempo, y lo que condujo al oro a subir, bajar y subir de valor a lo largo de un periodo de un par de años, en el caso del bitcoin se puede reducir todo a cuestión de meses o incluso semanas.

Después de la espectacular cotización que llegó a alcanzar el bitcoin en 2017 cercana a los 20 000 dólares, luego volvería a caer fuertemente, pero siempre muy por encima de lo que valía apenas un año antes a principios de 2017. La bola de nieve sigue rodando y realmente todavía no alcanzamos a imaginar el tamaño que habrá de llegar a tener.

LOS CAMINOS SE BIFURCAN

La popularidad creciente del bitcoin ejerció a su vez un efecto llamada, y esa bola de nieve adquirió su máximo tamaño a comienzos de 2018. Un fenómeno de este tipo afectó no solo a la cotización del bitcoin, sino al mercado de criptomonedas en su globalidad, ya que los inversores iban descubriendo unas tirando del hilo de las otras.

No hemos entrado todavía nosotros en el terreno de las *altcoins*, las otras criptomonedas existentes, y cuya aparición paulatina a lo largo de la evolución descrita hemos de momento esquivado. Quiero dejar el tema, de notable importancia, para más adelante, pues tiene mucho que ver con lo que existe de fondo bajo el Bitcoin, su tecnología y su potencial futuro.

El caso es que el bitcoin y las criptomonedas alcanzan ya un volumen de mercado a principios de 2018 de 500 miles de millones de dólares; un tamaño de

mercado que implica que la cosa tiene ya cierta relevancia en el contexto de la economía global. Por supuesto, es un peso específico todavía lejos del que ocupa el oro o grandes empresas como Apple o Google que valen varias veces más que todo el bitcoin existente en el mundo, pero en cualquier caso es ya significativo.

Esta subida exponencial del año 2017 ha provocado que muchos hablen de burbuja, pero creo que hay que poner las cosas en perspectiva. Lo que se ha vivido con el bitcoin es que, en su corta existencia, ha experimentado el mayor incremento de valor visto jamás en ningún activo financiero, disparándose en un periodo de tiempo muy breve. Para entender todo esto hay que tratar de ver cómo de grande es el bitcoin en términos relativos, en relación con otros activos financieros, y si realmente este tamaño se justifica o no. Si creemos que esto va a terminar reemplazando al oro y potencialmente a las monedas de nuestro sistema monetario fiduciario, su valor hoy por hoy es, en realidad, muy pequeño —en la última parte de este libro nos fijaremos realmente en cuál es el lugar que ocupan el bitcoin y el universo cripto en el conjunto de la economía—.

Lo que sí que trajo consigo ese 2017 con tal incremento acelerado en el valor de bitcoin y en el flujo de transacciones, fue la posibilidad de que se hicieran especialmente patentes algunos problemas de escalabilidad —cuestiones que atañen al número de transacciones, tamaño y periodicidad de transmisión de los bloques, rapidez, seguridad, robustez de los monederos, costes…—, y que se activara un debate en la comunidad sobre el rumbo que se había de seguir.

Las consecuencias son que, por un lado, donde en el bitcoin se detectan carencias, otras blockchains o criptomonedas encuentran su campo de actuación; y por otro, que dentro de la propia comunidad Bitcoin se manifiesten posturas enfrentadas acerca de cómo seguir evolucionando y escalando.

Para algunos lo más importante era seguir garantizando y reforzando las características identitarias de la moneda como descentralizada, pública, y resistente a las intervenciones externas y la censura; para otros, había que apostar por agilizar transacciones más rápidas y pagos con menos coste. No es que ambas facciones no desearan esos aspectos para el Bitcoin, era más bien una cuestión de prioridades y de interpretaciones diferentes sobre lo que habría hecho Satoshi Nakamoto ante tal dilema.

Y es así como se produjo la primera bifurcación —*fork*—, un concepto importante en la evolución de las criptomonedas y que proceden del software abierto u *open source*. En el mundo del *open source,* los *forks* o bifurcaciones vienen a ser el proceso por el cual un grupo de programadores decide coger un proyecto de código abierto —y, por lo tanto, con acceso al código fuente del

programa— y separarlo del original para seguir desarrollándolo con otro tipo de filosofía o funcionalidad.

En el mundo de las criptomonedas, que al final se pueden interpretar como dinero *open source*, el concepto de *fork* consiste básicamente en lo mismo. Un grupo de programadores deciden separarse de la línea de desarrollo de la moneda original y continuar con el desarrollo de la misma en otra dirección, heredando la historia hasta el punto de la bifurcación, pero convirtiéndose en otra moneda alternativa.

En el caso del bitcoin, y a falta de un Nakamoto que tomara decisiones, las dos facciones proponiendo diferentes soluciones de escalabilidad no se pusieron de acuerdo y se produjo un *fork* en verano del 2017. Lo que hasta ese momento había sido el bitcoin original pasó a convertirse en dos criptomonedas diferentes: Bitcoin —BTC o Bitcoin Core como se refieren a ella algunos— y Bitcoin Cash (BCH). Los primeros fueron los que querían una moneda que se mantuviera fiel a esa política de descentralización inicial; los segundos fueron quienes querían una moneda más ágil y barata a la hora de hacer pagos —de ahí el sobrenombre de *cash*, dinero en metálico— aun a coste de un posible incremento en la centralización de los mineros, lo cual resta capacidad de resistencia e independencia a la red.

La bifurcación, como explicábamos, significó que se tomaba el registro de toda la historia de bitcoin, con todas las transacciones realizadas hasta ese punto, pero en un momento dado ese registro se detiene, y aunque el Bitcoin sigue su camino, aparece una criptomoneda nueva —el Bitcoin Cash—, que a su vez continúa su camino por su lado. A quienes lo desearon, se les cambiaron sus bitcoins por bitcoins cash y de este modo pasaron a existir dos criptomonedas distintas, dos blockchains y dos comunidades diferenciadas de mineros.

Con esto se ponen de manifiesto algunos problemas o cuestionamientos que se han ido detectando en la historia particular del bitcoin, así como la existencia de otras criptomonedas alternativas que ofrecen prestaciones algo modificadas.

El universo cripto se ha expandido y se introducen nuevas variables en la ecuación. Y es que la auténtica revolución que nos ha traído el bitcoin no se agota en él, sino que reside en la tecnología y filosofía que subyacen bajo él, y que nos pueden llevar mucho más allá de esta moneda en concreto. De esto vamos a hablar a continuación.

SEGUNDA PARTE
LA NUEVA INTERNET DEL VALOR

4
BLOCKCHAIN: LA MAGIA TECNOLÓGICA DETRÁS DEL BITCOIN

Si nos hemos detenido en explicar qué es el bitcoin, cómo surgió, sus elementos definitorios y cómo está evolucionando es porque lo que consiguió hacer nuestro protagonista fue «irrumpir para disrumpir», nacer con vocación de provocar una revolución que fuera más allá de su exclusivo ámbito de actuación. Una revolución que está ahora mismo en marcha y se sustenta sobre unos pilares muy poderosos. El bitcoin ha funcionado como ha funcionado no solo por sus buenas intenciones —que se hubieran quedado en eso, en una declaración de intenciones —, sino por algo con mucha más proyección: la tecnología que lo sustenta.

Como ya anticipábamos en la Introducción, la dimensión esencial en el éxito del bitcoin lo constituye la tecnología que está detrás, la que hizo posible su nacimiento, la que ofrece unas posibilidades que van más allá de una transacción financiera y la que nos va a permitir ser testigos de muchas otras cosas que todavía están por llegar. Una «magia tecnológica» que es donde para mí reside el verdadero potencial disruptivo y revolucionario de esto, y no en ese juego especulativo que tanto interés está despertando.

A lo que me estoy refiriendo es a la tecnología blockchain —que todavía no fue así denominada en el texto fundacional de Nakamoto—, la cual se ha convertido en un versátil actor capaz de actuar más allá del escenario del bitcoin.

Es bien cierto que, en cualquier caso, todavía hoy blockchain se identifica de una manera estrechamente vinculada a bitcoin y, por extensión, también se asocia de forma injusta a ese fantasma de burbuja y especulación que sobrevuela en torno a la criptomoneda. Pero el potencial de blockchain es más que el bitcoin, y eso es lo que trataré de hacer ver en las siguientes páginas.

De lo que no cabe ninguna duda es que Bitcoin fue la primera cadena de bloques y la que marcó la pauta de funcionamiento de lo que sería la tecnología blockchain. Tal es así que podemos afirmar que, al explicar y conocer la

definición y elementos del bitcoin en los capítulos anteriores, estábamos asimilando, por extensión, el conocimiento de lo que significa y de cómo funciona toda esa nueva tecnología que habría de llamarse blockchain.

Aunque lo de «nueva tecnología» habría que matizarlo. Lo curioso es que en realidad el bitcoin no es una tecnología radicalmente nueva, sino la agregación de conceptos y tecnologías que ya existían, como redes P2P, técnicas criptográficas para realizar intercambios seguros, nodos… De hecho, las propias monedas digitales anteriores que llegaron a plantearse pero no a desarrollarse nunca —B-money y Bit Gold—, ya manejaban los mismos conceptos tecnológicos —como el uso de las funciones de *hash* para el algoritmo de consenso en el caso de B-money, o el concepto de una moneda digital completamente descentralizada en el caso de Bit Gold—.

Sabido es también que ya existían sistemas y protocolos P2P descentralizados que tuvieron su impacto en el campo del almacenamiento distribuido y en la compartición de información, especialmente de carácter audiovisual: desde Napster hasta BitTorrent, pasando por eDonkey o Gnutella. Eso sí, salvo en casos, todos los sistemas necesitaban, de alguna manera, un servidor centralizado para poder dar la funcionalidad que servían a los usuarios.

La verdadera gracia del modelo tecnológico que proponía Bitcoin radicaba en cómo juntar todos los elementos necesarios y conseguir que la agregación funcionara. En cierto modo es similar a lo que hizo Apple con el iPhone, ya que cuando salió al mercado no es que ofreciera ninguna tecnología que no existiera de antes —las pantallas táctiles, por ejemplo, ya se conocían, así como los móviles con GPS o con aplicaciones—, pero fueron capaces de ensamblar toda una serie de elementos distintos y conseguir así algo realmente innovador, para al final darle una funcionalidad revolucionaria. El caso de la tecnología blockchain que implantó Bitcoin es similar.

A diferencia de los intentos previos de otras monedas digitales como B-money o Bit Gold, bitcoin sí que fue la primera en conseguir combinar y aplicar esas tecnologías existentes para crear una criptodivisa digital con la que hacer posible la descentralización total de las transacciones electrónicas entre particulares de forma segura, evitando, además, ese habitual quebradero de cabeza para las entidades bancarias en cuestión de transferencias electrónicas del doble gasto.

Y algo así lo consiguió, como ya sabemos, mediante un libro mayor de contabilidad distribuido, que es lo que en realidad es una blockchain, o de forma más general, una base de datos distribuida formada por cadenas de bloques que han sido diseñadas con el fin de evitar su modificación una vez que un dato ha

sido publicado en el libro mayor o la base de datos. Es decir, que los datos son inmutables —o incorruptibles— y que la blockchain puede ser programada no solo para almacenar transacciones —como en el caso de bitcoin—, sino cualquier cosa que represente valor. Esa vendría a ser la definición, más o menos técnica, de blockchain.

Como se deduce de la misma, se trata de una tecnología especialmente adecuada para almacenar de forma creciente datos ordenados en el tiempo sin posibilidad de modificación ni revisión y sin necesidad de una entidad centralizada que garantice la integridad y la inmutabilidad de los mismos. Eso se lleva a cabo con procedimientos bien definidos en relación con el almacenamiento —que se logra replicando la información de la cadena de bloques—, transmisión —mediante redes de pares— y confirmación de la validez datos —a través del consenso entre los diferentes nodos participantes en la red distribuida—.

Hay que decir que Bitcoin nació con la vocación de ser una blockchain pública, es decir, sin restricciones para leer los datos de la cadena de bloques o para enviar transacciones que hubieran de ser incluidas en dichas cadenas, y sin ninguna restricción sobre quién pudiera participar de la misma. Su objeto inicial fueron las transacciones financieras —de hecho, eso sigue siendo determinante para que las transmisiones de datos sigan llamándose transacciones—, pero lo cierto es que una blockchain también puede ser privada, y los datos objeto de transmisión no tienen por qué ser solo transacciones financieras. Aquí es donde comenzamos a ampliar el espectro de posibilidades con respecto a esta tecnología.

No quiero extenderme en explicaciones técnicas mucho más porque ya aclaramos antes los elementos y funcionamiento de Bitcoin, el cual en esencia es aplicable a la generalidad de la tecnología blockchain. Ahora lo importante es identificar dónde reside lo verdaderamente revolucionario de esta tecnología, así como darnos cuenta de que sus posibilidades son de enorme calado.

Estamos llegando a la idea clave, al concepto que puede titular esta transformación revolucionaria y servir de nomenclatura a una nueva era: la de la Internet del valor. Porque eso es lo que está ocurriendo; blockchain está permitiendo trasladarnos de la Internet de la información a la Internet del valor.

Como ya hemos explicado antes, hasta la irrupción de la tecnología blockchain, en Internet se manejaban protocolos que permitían intercambiar información de muy distinta índole: ficheros, e-mails, páginas web, imágenes, vídeos, audios, voz… Eso es la Internet de la información, del contenido, de las

comunicaciones…, la Internet que usamos todos nosotros cada día y en la que han triunfado empresas que básicamente se dedican a eso, a transmitir información, contenido y comunicaciones, como pueden ser Google o Facebook.

Hay que decir que estos actuales gigantes han alcanzado este éxito en buena medida a costa de que los actores tradicionales que intermediaban en ese espacio como los medios de comunicación o las empresas de telecomunicaciones dejaran de tener el monopolio de esos activos, de la información y la comunicación, y que se expandieran las posibilidades de publicar contenidos y comunicarse de forma global a través de unos protocolos que evitaban que fueran necesariamente centralizados. Eso es lo que consiguieron, por ejemplo, WhatsApp o Skype, que se apoyan en determinados protocolos de Internet para la mensajería o la voz; o lo que hacen Google y Facebook con los contenidos. Es decir, se produjo un proceso de desintermediación que afectaba a cómo acceder a la información, al contenido o a las comunicaciones, y que dio paso a nuevos protagonistas que antes no existían.

Para el usuario final, esto ha tenido dos consecuencias mucho más importantes: por un lado, al introducir competencia en situaciones monopolísticas, se ha acelerado la innovación y, por lo tanto, ha mejorado la calidad de los servicios de forma exponencial —no hay más que comparar WhatsApp con el SMS, por ejemplo—. Y finalmente, la introducción de los actores ha permitido abaratar de forma significativa el coste para el usuario último de esos servicios hasta el punto de hacerlos prácticamente gratis.

Asimismo, blockchain permite dar el paso hacia la Internet del valor, ya que garantiza de forma segura y descentralizada la transmisión de dinero, y de forma más amplia, de valor y confianza, que es algo que tradicionalmente solo podía hacerse con la intermediación de las entidades financieras, los notarios, los abogados… Pero ahora hemos venido a contar con una especie de «tercero de confianza virtual». Nada menos.

Transmitir valor de forma descentralizada, segura y con confianza es algo revolucionario y con potencial para transformar todo el sistema financiero tal y como lo conocemos, y por extensión otros muchos sectores de actividad y la economía global.

Hasta ahora, para intercambiar dinero de forma segura, necesitábamos un intermediario como un banco. Ahora un individuo puede mandar bitcoins a otro de forma segura y fiable sin necesidad de nadie, excepto de la red descentralizada de Bitcoin para validar y aceptar la transacción. Y como veremos más adelante, esto se puede generalizar y transferir a otras formas de valor más

allá de las monedas, como acciones de empresas, propiedades inmobiliarias, etc. O incluso se puede ir todavía más lejos y tener aplicaciones distribuidas y descentralizadas, algo que más adelante explicaremos.

Imagina un Uber o un Airbnb donde el acceso a los taxistas o el alquiler de un apartamento para una estancia se haga de forma descentralizada, pero segura y confiable, en una red de blockchain pública sin un Uber o Airbnb que intermedie con la transacción. Ahí está la verdadera revolución de blockchain, y es por eso que muchos dicen que el futuro es descentralizado.

Por todo esto estoy convencido de que blockchain representa la nueva generación de Internet y que el mundo va a cambiar de manera radical en los próximos años gracias a esta tecnología disruptiva, tal y como el e-mail cambió el correo tradicional.

Sus posibilidades, además, van más allá del sector financiero. Desde que Bitcoin pusiera en funcionamiento este planteamiento tecnológico que crea un nuevo protocolo en Internet, ha dado comienzo una carrera en muchos ámbitos por la aplicación de esta innovación de la manera más eficiente posible y con distintos usos. Se abre el abanico de posibilidades y aplicaciones, y algo de eso hemos de debatir en las próximas páginas, ya que resulta más que evidente que blockchain se ha convertido en nuestro mejor candidato para desencadenar una nueva revolución tecnológica.

Pero antes de adentrarnos en las posibilidades de blockchain, veamos cuál ha sido la evolución de las criptomonedas.

5
CRIPTOMONEDAS ALTERNATIVAS: LOS HERMANOS Y PRIMOS DEL BITCOIN

Bitcoin (BTC) fue la primera criptomoneda y la primera blockchain, pero, como acabamos de decir, esta tecnología admite otras posibilidades, entre las cuales está el ser aplicada en la emisión de nuevas criptomonedas diferentes al propio bitcoin, empleando otros algoritmos y dotándolas de otras propiedades, aunque generalizadamente con los mismos principios de uso de una red de P2P descentralizada, inmutabilidad y de transacción electrónica segura. Es así como surgen otras criptomonedas, las llamadas *altcoins* o monedas alternativas.

Pasaron dos años desde que nació el bitcoin sin que se registraran novedades en este terreno, pero en el año 2011 comienza ya a registrarse movimiento en este sentido, fruto del incremento de popularidad que empieza a adquirir la criptomoneda pionera.

Algunas de las primeras divisas digitales fueron Namecoin y Litecoin, pero en la actualidad hay decenas de criptomonedas en circulación y constantemente aparecen otras, si bien los casos de éxito relevante son bastantes menos. Lógicamente, cada criptomoneda trata de mejorar alguno de los aspectos del diseño original de Bitcoin relativos a su escalabilidad, velocidad, anonimato, u otra posible ventaja, o bien ofrecer usos distintos o aplicables en nuevos contextos. Veamos un poco su historia y las más relevantes.

NAMECOIN (NMC)

Namecoin (NMC) fue la primera criptomoneda que apareció. Lo que intentó fue usar la blockchain de Bitcoin, pero aplicada a los dominios de Internet —esos que conocemos todos como .com, .es, .net, etc.— para que fueran, como ya

se había logrado mediante esta tecnología con el dinero digital, también resistentes a la censura.

Hay que saber que estos dominios son concedidos por una entidad central y hay una serie de servidores distribuidos por el mundo —los llamados servidores de DNS o *Domain Name System*— que traducen las direcciones de url, nombres y dominio, en direcciones de IP para que los usuarios puedan acceder a los servidores que proveen de los servicios relacionados con esos dominios. En caso de resultar atacados estos servidores, podría dejarse sin acceso a Internet a los usuarios, ya que los navegadores no podrían acceder a los servidores de los servicios al no poder traducir los nombres de los dominios en direcciones de IP físicas para accederlo. En 2016 un ataque a muchos servidores de DNS dejó a los usuarios sin acceso a Twitter, Amazon, Spotify y otros servicios durante unas horas.

Nos hallamos, pues, ante una extensión de los posibles usos que se le ha concedido a la tecnología blockchain y que consiste en permitir proteger los dominios de Internet de este tipo de ataques. Es así como se ha creado el dominio .bit, completamente descentralizado. El registro sin censura alguna de este dominio se ha convertido, por lo tanto, en la función principal de Namecoin.

LITECOIN (LTC)

Otra de las primeras criptomonedas fue Litecoin (LTC), cuyo nombre deriva del término *light*, es decir, 'ligero' en inglés, lo cual ya nos advierte de cuáles fueron sus intenciones desde el principio.

Fue creada por Charlie Lee, antiguo empleado de Google, que percibió los problemas de escalado que podía padecer Bitcoin tal y como estaba configurada. Recordarás que esto ya lo hemos hablado en un capítulo anterior, que fue algo que se puso de manifiesto en 2017 y que condujo a la bifurcación entre Bitcoin (BTC) y Bitcoin Cash (BCH).

Digamos que, de algún modo, Charlie Lee lo había previsto años antes. Por ello creó una nueva criptomoneda modificando el algoritmo de Bitcoin, de manera que resulta prácticamente idéntica en lo técnico, pero con unas diferencias significativas en lo que se refiere a esa «política monetaria» que describíamos en su momento, y que afecta a la cantidad de monedas que hay que emitir y al tiempo de procesamiento de los bloques.

Lee consideró que la emisión de un bloque cada diez minutos, una vez que hubiera muchas transacciones, provocaría que, dadas las limitaciones de tamaño de los bloques de Bitcoin —el mayor centro del debate entre los partidarios de Bitcoin y Bitcoin Cash—, las transacciones pendientes no iban a caber en un bloque y, por lo tanto, en lugar de ser verificadas en diez minutos, iban a tardar más porque se hacía necesario esperar a poder entrar en el bloque siguiente. De hecho, es lo que pasa hoy en Bitcoin y el motivo de por qué las transacciones tardan más de diez minutos en validarse.

Anticipando este problema, lo que Lee hizo fue reducir el tiempo de generación del bloque a dos minutos y medio en vez de los diez de Bitcoin, y modificó, asimismo, el propio algoritmo que se usa para llegar al consenso en la red y verificar las transacciones, facilitando la minería y no exigiendo así equipos tan sofisticados para tal fin.

Además, la red Litecoin habrá de producir aproximadamente cuatro veces más unidades que la de Bitcoin. Obviamente, cada criptomoneda que se cree tiene su autonomía para establecer su propia política monetaria y, evidentemente, si se emiten más, resulta también más atractivo dedicarse a minar porque hay más opciones de que te pueda tocar algo. No obstante, a su vez, esto reduce el valor de la unidad monetaria —luego cada cual establecerá sus criterios en ambos factores, aunque yo considero que sigue saliendo mejor financieramente la escasez de bitcoin y la mayor dificultad que exige su minado—.

El caso es que Litecoin consigue hacerse bastante popular por este motivo y, sobre todo, porque logra hacer las transacciones y verificaciones de manera más rápida, aunque a su vez pierda con respecto al Bitcoin potencial como almacén de valor, al ser más abundante y registrar más transacciones. El paralelismo que Charlie Lee establece entre ambas criptomonedas con el oro —más escaso— y la plata —más transferible— es directa: si Bitcoin es el oro digital, al Litecoin se le conoce como la plata digital.

Litecoin se ha caracterizado asimismo por ser una de las criptomonedas que más rápida y ágilmente es capaz de adoptar las nuevas tecnologías. Ejemplos de esto es la tecnología del *Segregated Witness* —o SegWit, que es como se conoce — que permite que las transacciones sean más rápidas y baratas —posibilita segregar cierto tipo de datos de las transacciones haciendo que quepan más en cada bloque y, por lo tanto, se validen más transacciones de golpe—, o del *Lightning Network*, que básicamente permite que se hagan transacciones muy rápidas, pero fuera de la blockchain, para luego ser introducidas en esta sin perder seguridad. Son soluciones que abordan los tradicionales problemas de

escalado que padece Bitcoin, y que Litecoin puede integrar mucho más fácilmente dada la mayor rapidez de su comunidad y el menor tamaño y uso que tiene la misma.

La considerable agilidad que ofrece Litecoin, lo cual *a priori* no cabe verlo sino como positivo, nos permite plantear un debate que está candente en el mundo de las criptomonedas. En los procesos de creación de las mismas hay que tener en cuenta que estamos hablando de una tecnología, la blockchain, que basa su razón de ser en el hecho de buscar el consenso, por lo que cualquier cambio en el software que dé lugar a una nueva versión o nueva blockchain habrá de ser lento por necesidad, y debe aguardar a ser consensuado por la comunidad, esto es, por los desarrolladores, los mineros, las *exchanges*, etc. De partida podemos decir que los cambios no pueden hacerse rápido.

Sin embargo, también en este terreno Litecoin ofrece más agilidad, pues cuenta con una comunidad más pequeña y, en consecuencia, tiene la capacidad de adoptar los cambios de forma más rápida. Aquí es donde emerge la controversia, puesto que para muchos esto no es sino una nueva manera de acercarse a la centralización, perdiéndose el concepto identitario de partida. Ahora bien, la máxima descentralización y el hecho de que no haya nadie que tome las decisiones sin consensuar evidentemente ralentiza.

Una comunidad grande sin un líder claro —recordemos que Nakamoto desapareció en 2011— implica más lentitud. Por otro lado, Litecoin o Ethereum —de la que luego hablaremos— sí cuentan con unos líderes más visibles, claros e influyentes, y en el caso del primero se trata de comunidades más pequeñas, por lo que se permite una toma de decisiones más rápida, aunque se pierda descentralización. Este debate incidiría también en la bifurcación posterior de Bitcoin y Bitcoin Cash.

RIPPLE (XRP)

Otra de las criptomonedas más valoradas en la actualidad —ocupa la tercera posición por tamaño de mercado, y durante un tiempo fue la segunda, hasta la irrupción de Ethereum—, es Ripple (XRP). También es de las más controvertidas, puesto que se la considera «la criptomoneda de los bancos», y de hecho muchos argumentan que en realidad ni es una blockchain de verdad ni una criptomoneda.

Lo cierto es que la actividad como empresa de Ripple precede incluso a la de Bitcoin, ya que nació en el año 2004 bajo el nombre de Ripplepay, apuntando ya a la idea de dinero digital y de descentralización en sus transacciones, e incluso contaban desde 2005 con un software propio. Sin embargo, no fue hasta el año 2011, aprovechando ya el tirón de Bitcoin y las posibilidades tecnológicas de blockchain, que todo eso no se materializaría en algo realmente aplicable y valioso. El sistema de Ripple actual no tiene nada que ver con el que se desarrolló durante esta primera época y de alguna forma, en el año 2011, Bitcoin había triunfado donde Ripple no lo había conseguido: en desarrollar un sistema de dinero digital seguro y descentralizado mediante una red P2P.

El principal responsable de conseguir dar este paso en 2011 fue Jed McCaleb, que ya había sido el creador de eDonkey, y fue, además, también quien desarrolló la *exchange* MtGox antes de vendérsela a Mark Karpelès, y que actualmente es el fundador y responsable técnico de Stellar —una blockchain de tercera generación de la que hablaremos luego—, por lo que su trayectoria en el ámbito de las redes P2P y de las criptomonedas queda suficientemente atestiguada.

Tras la experiencia de MtGox, McCaleb se dedicó a crear su propia criptomoneda. Su principal interés era eliminar la prueba de trabajo de Bitcoin en la que se basa su proceso de minado, ese algoritmo que buscan resolver los mineros y que exige tanta capacidad de computación y consumo energético.

Es bajo esa premisa que se unió a los fundadores de Ripple, que en ese momento cambió su nombre a OpenCoin, y llegaría a asumir el liderazgo del nuevo proyecto, trabajando en la creación de un protocolo que permitiera la transacción de dinero, pero sin necesidad de minado. Para ello, aprovecha la tecnología de blockchain y la creación de una red de nodos, como en el caso de Bitcoin, pero sin que se produzcan operaciones mineras, tan solo transacciones verificadas por varias partes para lograr consenso.

Algo así se lleva a cabo haciendo que cada nodo de Ripple —los llamados *ripple gateways* que se lanzan alrededor de 2012— funcione en sí mismo como un sistema de cambio local, una especie de PayPal, aunque sin autoridad central, ya que ningún nodo tiene mayor capacidad que el resto. Estos *ripple gateways* no son nodos distribuidos y descentralizados en una red P2P, sino nodos sometidos a algún tipo de negocio establecido y controlados por una corporación.

Lo que esto permite es que se puedan conectar los sistemas de pago tradicionales y los alternativos en una sola red, y que sea posible la conversión

entre distintas divisas y criptomonedas. Además, al no haber operaciones de minado, las transacciones son mucho más rápidas que en Bitcoin. Por otro lado, la introducción de las *ripple gateways* elimina una de las principales características de una blockchain como la de Bitcoin, la descentralización. Es por este motivo que la comunidad cripto más maximalista no tiene ningún aprecio por la plataforma de Ripple, puesto que entienden que va en contra de la filosofía principal de las redes cripto.

En abril de 2013, Ripple lanza su infame criptomoneda, el XRP. Digo infame porque lo hacen con ciertas características que de nuevo no gustan nada a la comunidad cripto más ortodoxa. La criptomoneda XRP no tiene el concepto de minado, y Ripple —ya renombrado de nuevo de OpenCoin a Ripple Labs— emitió de golpe una cantidad desorbitada de las mismas —100 000 millones—, pero poniendo un porcentaje extremadamente pequeño a la venta y conservando ellos la amplia mayoría, así como dando 20 000 millones de monedas a los fundadores. También cabe decir que no estaba nada claro que hubiera ninguna necesidad de crear una criptomoneda como el XRP para el uso de la plataforma de Ripple, y de hecho hoy ese es uno de los puntos más controvertidos dentro de la comunidad: si de verdad XRP tiene algún valor intrínseco asociado a su futuro uso, o si su valor es estrictamente especulativo.

Por otro lado, no es de sorprender que las características de esta plataforma resultaran especialmente atractivas para el sector bancario, y entidades como el Banco Santander, el BBVA o American Express hayan invertido en la compañía Ripple y hayan empezado a experimentar con la tecnología para sí mismos, ya que se han dado cuenta de que puede resultar de enorme utilidad para resolver de manera más ágil su problema con el doble gasto, y en particular puede llegar a reemplazar el modo en que los bancos realizan las transacciones internacionales, hoy por hoy basado en el anticuado protocolo conocido como SWIFT y que es el responsable, entre otras cosas, de que enviar dinero internacionalmente sea muy lento para el mundo digital —cuestión de días, y no de minutos o segundos—.

De esta manera, Ripple se ha convertido en la blockchain privada por excelencia, la criptomoneda de los bancos, la que les permite realizar sus transacciones internas de forma rápida y segura. Obviamente, no es difícil darse cuenta de que Ripple no está muy bien considerada en la comunidad Bitcoin, porque supuestamente la idea de partida no era ayudar a los bancos, sino sustituirlos, y apostar por blockchains públicas, y no privadas.

Sin embargo, Ripple sí que se ha convertido en una criptodivisa muy popular entre los inversores, estimulados seguramente por el hecho de que los bancos

hayan apostado por la empresa, algo que les aporta confianza. No obstante, conviene tener en cuenta que las entidades financieras en realidad no están apostando por la criptomoneda, sino por tecnología que les ofrece y que, por lo tanto, Ripple puede llegar a ser muy valioso como empresa sin que su moneda XRP tenga ningún valor en absoluto, ya que una cosa y otra no están necesariamente vinculadas.

MONERO (XMR)

Si Ripple es la moneda más cuestionada en la comunidad Bitcoin, Monero (XMR) vendría a ser la alternativa a Bitcoin de los más «puristas», la de aquellos que cuestionan a la blockchain pionera porque no es cien por cien anónima, tal y como resultan las transacciones de dinero en metálico.

Hay que tener en cuenta que Bitcoin exige registros públicos que se basan en códigos o claves, y aunque no aparecen públicamente nuestros nombres, sí figuran nuestras identificaciones numéricas, la dirección identificativa de nuestro monedero digital, de modo que si uno llegara a averiguar la correspondencia entre nuestra persona y nuestro monedero, conocería todas nuestras operaciones. Es decir, Bitcoin es un sistema que busca el anonimato, pero que no llega a ofrecerlo al extremo de como sería posible en el caso del dinero en metálico. La criptomoneda Monero nació con el objetivo de actuar en este sentido, de buscar el anonimato más completo posible, siendo la privacidad su prioridad máxima.

Monero ofrece principalmente dos propiedades novedosas en el reforzamiento de esa privacidad. En primer lugar, las monedas en Monero son fungibles. ¿Qué significa esto? En Bitcoin cada moneda es única, y si sale de mi monedero al tuyo, yo ya no lo podré usar y tú sí. Y si ese bitcoin se mueve a su vez a otro monedero podemos «tracear» su historia, seguirle la pista, desde el día de su emisión a su última transferencia. Sin embargo, cuando decimos que en Monero las monedas son fungibles, queremos decir que, considerando mi monedero y el tuyo como iguales, queda registro de que ha habido una transacción, pero no se puede detectar de qué monedero ha salido y a cuál ha llegado. Es decir, sí que queda constancia de una transacción, pero es imposible saber entre quiénes se ha efectuado. Es como si los euros no tuvieran números de serie.

Por ello, Monero incorpora una tecnología específica para no poder hacer visibles las direcciones de los monederos. Se trata de un sistema muy sofisticado que ha conseguido mantener las propiedades de una blockchain de

inmutabilidad, contabilidad distribuida y alta seguridad, pero ocultar las transacciones y hacerlas realmente anónimas.

Monero también modifica el sistema de minado. Como ya sabemos, el minado de Bitcoin exige equipos muy especializados, alta capacidad de computación, alto consumo, etc. Hay incluso chips especiales para minar mejor, y todo esto hace que haya importantes barreras de entrada hoy en día. Desde Monero —no son los únicos— han diseñado un proceso de minado que invalida las ventajas de esos chips para democratizar este proceso y permitir que cualquier equipo pueda llevarlo a cabo. Esto, unido al anonimato máximo, ha convertido a esta moneda por un lado en la favorita de aquellos que quieren usar el dinero digital en negocios ilegales, y por otro, en el target favorito de *hackers*, que consiguen que la gente se descargue sin querer software específico en sus dispositivos para que les hagan minado de Monero sin que ellos lo sepan.

En el mundo del bitcoin, es práctica habitual poner en la lista negra ciertas direcciones que se sabe que contienen bitcoins que han sido conseguidos con actividades ilegítimas —*ramsonware*, *hacks*, etc.— para evitar que se puedan usar o vender, pero eso en Monero no es posible.

En definitiva, Monero recoge la filosofía de la privacidad y la descentralización y la lleva hasta el final, pero con ello también se convierte, como hemos visto, en la criptomoneda más atractiva para actividades ilícitas.

HACIA LA SEGUNDA GENERACIÓN

He querido explicar brevemente en qué consisten estas cuatro criptomonedas porque, aunque en la actualidad hay cerca de mil en el mercado, la citadas, además de figurar entre las más relevantes, ejemplarizan muy bien varios aspectos que están en el debate público que se mantiene en torno a la criptoeconomía: nuevos usos y utilidades, mejoras en la escalabilidad y rapidez, blockchains públicas *versus* blockchain privadas, mayor descentralización y privacidad, mayor democratización en el proceso de minado, etc.

A fecha de febrero de 2018, el listado de criptodivisas, ordenado según su valor en el mercado, sería el siguiente:

1. Bitcoin (BTC) (128 000 millones de dólares)
2. Ethereum (ETH) (74 000 millones)
3. Ripple (XRP) (29 000 millones)

4. Bitcoin Cash (BCH) (17 000 millones)
5. Cardano (ADA) (9000 millones)
6. Litecoin (LTC) (7000 millones)
7. Stellar (XLM) (7000 millones)
8. NEO (6000 millones)
9. EOS (5000 millones)
10. NEM (4000 millones)
Resto (70 000 millones)

En el listado identificarás alguna criptodivisa de la que todavía no hemos hablado, y te llamará especialmente la atención el hecho de que la blockchain más importante después del Bitcoin sea una tal Ethereum, y su criptomoneda ether (ETH) ocupe una privilegiada posición y un notable porcentaje de valor dentro del conjunto de la criptoeconomía. Y, sin embargo, todavía no hemos profundizado en ella. El olvido ha sido premeditado, ya que dada su importancia e influencia he considerado que merece un aparte, espacio más relevante.

Y es que las monedas de las que hemos venido hablando aportaron cada una alguna nueva dimensión a las posibilidades de Bitcoin y la tecnología blockchain, pero el verdadero salto cualitativo, el que iba a abrir nuevas vías de transformación en los mercados financieros, en el mundo empresarial, y en la economía en su conjunto, lo aportó esta nueva blockchain llamada Ethereum. Con ella podemos afirmar que llega la segunda generación de blockchain. Es necesario, en consecuencia y como hemos dicho, dedicarle cierta y especial atención, tanto a la plataforma en sí como a las nuevas posibilidades y elementos que ha traído consigo.

Asimismo, si con Ethereum vamos a conocer la segunda generación de criptomonedas, el listado nos enseña también otras que en estos momentos se sitúan bastante más atrás en su posición dentro de lo que representan en la capitalización del mercado, pero que se cuelan también dentro de ese *top ten*. Vendrían a ser las llamadas plataformas blockchain de tercera generación. Nos referimos a Cardano, Stellar, NEO, NEM o EOS, de las que hablaremos en la última parte de este libro.

6
ETHEREUM: LLEGA LA BLOCKCHAIN 2.0

DINERO PROGRAMADO

En el año 2014, en un momento de plena efervescencia en cuestión de aparición de nuevas criptomonedas, nació la plataforma de blockchain pública Ethereum. Pronto se comprobó que esta no era una más. Ethereum no se limitaba a cambiar en algo el algoritmo de Bitcoin y mejorar alguna propiedad o priorizar determinada prestación para crear otra criptomoneda. Fue mucho más allá al ser capaz de permitir nuevas posibilidades de programación en los nodos de la cadena de bloques.

La tecnología que ofrecía era bastante más potente que lo visto hasta ese momento, y su contribución a la criptoeconomía estaba llamada a ser francamente revolucionaria, puesto que superaba el ámbito estricto del dinero digital y entraba de lleno en el concepto de propiedad digitalizada y de las aplicaciones descentralizadas o *Dapps*, lo cual abría muchísimas posibilidades en los mercados, ofreciendo innovadoras maneras de financiar y monetizar proyectos empresariales y digitalizar la propiedad, así como vías muy poderosas para proporcionar liquidez. Esto ocurría en buena medida gracias a la introducción o popularización de esta plataforma de los *smart contracts* —o contratos inteligentes— y de las ICO, que se extendían a ritmo exponencial en infinidad de actividades de carácter financiero o empresarial.

Detrás de Ethereum está un programador de origen ruso canadiense llamado Vitalik Buterin, nacido en 1994; es decir, que apenas tenía veinte años cuando creó esta revolucionaria plataforma. Sigue siendo muy joven ahora, pero su juventud no le ha impedido convertirse en una de las primeras figuras en el mundo de cripto y blockchain. Lo cierto es que desde los diecisiete Buterin estaba volcado por completo en el universo del bitcoin y se dedicaba

constantemente a escribir sobre esta materia. Él fue quien fundó en 2011 la *Bitcoin Magazine*.

Buterin se dio cuenta de que existía la posibilidad de generalizar lo que hacía Bitcoin mediante su red distribuida y descentralizada de contabilidad y de registros inmutables a otras funcionalidades. Por ejemplo, una red descentralizada de computación donde se pudieran ejecutar aplicaciones.

La mayoría de las aplicaciones que conocemos pasan hoy por un servidor que se encarga de llevar a cabo la computación con los datos que recibe, e inmediatamente proporcionar un resultado. Este es el caso, por ejemplo, de WhatsApp: el mensaje que tú emites pasa por su servidor, y luego este se encarga a su vez de emitirlo. Se trata de una red P2P, pero no estrictamente descentralizada, puesto que hay alguien en medio que se asegura de que esa transacción se realice.

Lo que pretendía Buterin —y conseguiría con Ethereum— era desarrollar aplicaciones descentralizadas del todo; es decir, donde la red en sí misma fuera la que ejecutara y validara la aplicación, la entrada y la salida, y le llegara a quien estaba al otro lado sin que hubiera un punto centralizado que tomase la decisión de cómo ejecutar dicha aplicación. Se trataba de un tipo de computación diferente al que conocemos, pero sin duda representaba el futuro, la manera en que muchas aplicaciones se desarrollarían a partir de ahora.

Sin embargo, el lenguaje de programación de Bitcoin era un tanto limitado y no permitía que a las transacciones que se registran en los nodos se les pudieran añadir o programar otras propiedades. Por ello en 2013 publicó un artículo en este sentido, comunicando que era posible aumentar la plataforma de Bitcoin de forma que se permitiera que los nodos tuvieran esa capacidad de programación y pudieran añadir nuevas propiedades. Estaba anticipando la red de aplicaciones descentralizada y, de algún modo, lo que estaba ya solicitando es que el dinero fuera programable, que las capacidades de los nodos no se limitaran solo a registrar las transacciones que incluían cada bloque.

Las ideas de «red de aplicaciones distribuidas» y de «programar dinero» eran, sin duda, disruptivas, pero no obtuvieron ninguna receptividad en su momento dentro de la comunidad bitcoin. Como ya sabemos bien a estas alturas, esta comunidad funciona como la mayoría de las comunidades de software abierto y si no hay consenso entre los programadores principales para aceptar un cambio, este no se hace. Y en este caso hubo bastante poco.

Es por ello que en enero de 2014, Vitalik Buterin anunció que iba a crear una nueva blockchain capaz de ejecutar no solo transacciones, sino también

aplicaciones de forma distribuida y descentralizada. La llamó Ethereum, un término procedente del ámbito de la ciencia ficción que alude al medio invisible que permite que se pueda viajar a la velocidad de la luz en el universo. Pero lo que traía consigo no era algo de ciencia ficción, aunque pudiera parecerlo por su carácter tan innovador, sino una realidad inminente: había nacido la que estaba llamada a ser la tecnología más disruptiva desde que lo había hecho Bitcoin.

PROPIEDADES DIGITALIZADAS Y APLICACIONES DESCENTRALIZADAS

El proyecto de Ethereum se materializó en una fundación afincada en Suiza, desde la cual Buterin lideró un equipo encargado de desarrollar esta nueva plataforma y crear su propia criptomoneda, el ether (ETH), que es lo que se mina para que haya un incentivo económico para formar parte de la red, al igual que en el caso de Bitcoin, pero que es a su vez la moneda con la que se paga por el uso de la plataforma de Ethereum. Así, el valor del ETH debería estar altamente correlacionado con el uso que se haga de Ethereum como plataforma de block-chain. Otro aspecto interesante del ETH es que, al contrario del bitcoin, no tiene una política monetaria deflacionaria y no tiene determinado el número máximo de ETH que sean emitidos.

La gran aportación de Ethereum fue que permitió programar los nodos para que se ejecuten programas de software completos, pero siempre de manera distribuida, es decir, con las mismas propiedades que las transacciones de bitcoins —descentralizadas, imposible de ser censuradas, seguras, el código es inmutable, etc.—.

Estos programas que se ejecutan son los llamados *smart contracts* o contratos inteligentes, un paso adelante decisivo, puesto que la integración de esta modalidad algorítmica en blockchain, el poder «programar dinero», ha permitido abrir la puerta al desarrollo de infinidad de aplicaciones prácticas, y dar el paso hacia una nueva realidad: la digitalización de la propiedad.

De forma muy sencilla, un contrato inteligente es un programa de software que se ejecuta normalmente junto con una transacción financiera. Básicamente, un contrato inteligente es un programa que dice «si pasa A entonces haz B», donde A es algún tipo de evento y B muchas veces es un pago. Por eso se llaman contratos y no programas. Una de las grandes ventajas de estos contratos

inherentes a blockchain es su seguridad e inmutabilidad, no se pueden alterar ni modificar.

Si Bitcoin creó el dinero digital, podemos concederle a Ethereum la creación de la propiedad digitalizada, puesto que su tecnología permite codificar las propiedades de un activo mediante un contrato inteligente. Por ejemplo, si yo quiero comprar un coche a plazos, puedo crear un *smart contract* que gobierna cómo ocurren las cosas: establece la adquisición por mi parte de ese activo, y programa la transferencia de dinero periódica de mi monedero al monedero del vendedor en los términos y plazos que hayamos acordado.

Precisamente, como el contrato es inmutable, no puedo modificarlo para dejar de pagar o cambiar la cantidad que tengo que pagar, y se ejecuta de forma automática —es como una transferencia de banco periódica pero descentralizada —. Esto, como seguramente ya empiezas a ver, tiene muchísimas posibilidades ya que, en general, en cualquier entorno en el que haya que confiar en alguien concreto para que algo pase —un seguro, una hipoteca, una apuesta, cobrar un sueldo, un dividendo, etc.—, se puede automatizar y eliminar al intermediario que provee de esa confianza —y cobra por ello— a través de este código informático auditable, completamente transparente y no manipulable por ninguna de las dos partes.

Si vamos un paso más allá, una *Dapp* o aplicación descentralizada, es básicamente una aplicación de usuario final —una app móvil o una web— que interacciona con la blockchain de Ethereum —u otras, como ya veremos— mediante una serie de *smart contracts*. Las *Dapps* suelen usar también almacenamiento distribuido y el código fuente suele estar abierto.

Veamos un ejemplo de cómo funcionaría DUber o un Uber descentralizado. En este escenario habría una aplicación de código abierto DUber que sería lo que se usaría por parte del usuario final para pedir un taxi. La relación entre el app DUber y los taxistas está gobernada por un contrato inteligente que especifica cómo se pagan los taxis, qué comisiones hay involucradas o cómo cambian las tarifas, todo de forma descentralizada y transparente —no como hoy en día, que no se sabe exactamente el criterio por el cual Uber con frecuencia sube los precios, teóricamente para atraer más conductores—.

Esto tiene bastantes ventajas. Primero, se elimina el intermediario y, por lo tanto, se abaratan los costes y se reducen las comisiones. Segundo, se provee de transparencia al sistema y posiblemente un reparto más equitativo del valor generado. Por último, es mucho más rápido, sencillo y barato de implementar que la versión centralizada. Enseguida veremos, además, cuando expliquemos

los tokens, que, con estas aplicaciones, e introduciendo un token como criptomoneda dedicada para el consumo de estos servicios descentralizados, podemos llegar a conseguir que una parte importante de los 60 000 millones de dólares que vale Uber hoy, se hubieran repartido entre los taxistas y los usuarios de DUber, y no todos hubieran ido a parar a la empresa que controla el servicio y sus inversores. Es decir, hubiéramos también descentralizado el valor que ha creado Uber como empresa.

Como acabamos de comentar, muy ligado a esta idea de digitalizar la propiedad y de las aplicaciones descentralizadas está el concepto de token, que también trae consigo Ethereum, ya que su tecnología y programación nos permite crear algo que no sea necesariamente una moneda, sino también otros tipos de representación de utilidad o valor.

Los tokens son, por un lado, criptomonedas —el bitcoin puede ser interpretado como el primer token digital que se creó—, que como todas las que venimos citando se pueden gestionar sin la necesidad de un banco central. Al igual que bitcoin o ether, estos tokens están en la blockchain, se guardan en monederos y se pueden comprar o vender en las *exchanges*, o conseguir por otros medios. La gran diferencia es que estos están vinculados a un contrato inteligente que define cómo funciona el token, cuál es su política monetaria —o sus *token economics* como se conoce en la industria—, cómo y dónde se puede usar, etc. En esencia es como poder lanzar una criptomoneda programable, pero por encima de una blockchain que ya existe, en este caso Ethereum. Además, para un desarrollador experimentado crear un token para un proyecto es extremadamente sencillo.

Veamos dos tipos de tokens, empezando con los más populares hoy, los conocidos como *utility tokens* o tokens de utilidad, que es el que podría usarse dentro de un ecosistema particular si se quiere participar de determinados servicios que ofrezca.

Podemos hacernos una idea de lo que significa esto si atendemos al funcionamiento los casinos, algunos festivales de música o Disneylandia. Como todos sabemos, los casinos emiten sus fichas —sus tokens—, que son los que funcionan dentro de los mismos como representación del dinero a la hora de apostar. En Disneylandia lo que existe es una pulsera electrónica que cargas y que te permite realizar los pagos de las atracciones y consumiciones dentro de su recinto, dentro de su ecosistema. Entre los festivales de música hay experiencias tanto de tokens propios como de pulseras electrónicas.

Los tokens de los que venimos hablando en relación con la criptoeconomía son algo similar. Se trata o bien de derechos de uso de una plataforma o bien de servicio concreto —como el caso del token del casino o de Disney—, que es lo que se correspondería con el token de utilidad.

La idea es que si la política monetaria del token está diseñada correctamente y el negocio de los casinos, de los festivales de música o de Disney —aquellos donde solo se puede funcionar o consumir con su token propio— crecen de forma más rápida que la emisión de tokens nuevos, el valor de este no puede más que subir de precio para poder acoger a los nuevos consumidores de esos tokens.

También se podrían usar como incentivo para mejorar los negocios. Por ejemplo, Disney podría darlos como reclamo a que ciertos restaurantes se establecieran en Disney y de esa forma incentivarles a hacer que Disney en general fuera bien, ya que en ese caso no solo su negocio iría también bien, sino que el valor de sus tokens subiría. En cierto modo puedes ver el símil con los mineros de Bitcoin y cómo tienen un incentivo económico —reciben bitcoins por estar en la red—. Es lo mismo, pero con muchísima más aplicabilidad en multitud de negocios.

Volviendo al ejemplo de DUber, en un entorno descentralizado es más complicado cobrar comisiones por intermediar y, por lo tanto, las empresas que lanzan esos servicios tienen que buscar otros modelos de negocio. Una posibilidad sería la creación del token DUber. Este serviría como moneda de pago de los servicios de los taxistas, y tendría un contrato inteligente asociado que permitiría hacer estos pagos de monedero de consumidor a monedero de conductor de forma automática. Pero no solo eso. DUber podría haber dado tokens DUber tanto a los futuros usuarios del servicio como a los taxistas y a sus empleados, de forma que ahora habría un incentivo económico alineado entre los tres constituyentes del negocio: los que desarrollan el servicio, los que lo consumen y los que lo prestan.

Si el negocio va bien y el consumo sube, también lo hace el valor del token y todos ganan. Algo nunca visto. En la economía tradicional las empresas suelen estar desalineadas en sus incentivos e intereses frente a sus diferentes constituyentes. Por un lado, los accionistas quieren más beneficios, lo cual ejerce presión al equipo gestor de la empresa para que suba precios y baje costes. Por otro, los clientes quieren mejor servicio a menor coste y los empleados quieren mayor compensación, lo cual implica más costes. Imposible contentar a todo el mundo y normalmente los que se suelen salir con la suya al final son los dueños, es decir, los accionistas.

En un servicio descentralizado monetizado vía tokens, todo el mundo está incentivado en remar en la misma dirección. Mejor servicio, más barato, más usuarios lo adoptan, más sube el token de valor y más ganan todos —siempre y cuando la política monetaria y de distribución del token esté correctamente diseñada—.

Otra alternativa de los tokens es que sean representaciones digitales de activos económicos y representen un valor dentro de un negocio con los derechos subyacentes —por ejemplo, dividendos—, que es lo que se conocería como token securitizado o *security token*. Pueden ser asimilables a las acciones de una empresa, pero también representar activos como propiedades inmobiliarias u obras de arte, de manera que, además de acciones, tienen ingresos o beneficios, o un dividendo, o cualquier otro derecho económico. Como definíamos antes, lo que permiten es digitalizar la propiedad.

Estos token pueden asimismo listarse en las *exchanges* existentes, igual que las criptomonedas, y cotizar y permitir operaciones de compraventa de ellos, con lo cual tienen otro gran valor añadido, que es el de proveer de liquidez al activo subyacente.

Además, los tokens son muy fáciles de crear; y desde que se popularizó el concepto en 2014 o 2015, ya han salido al mercado infinidad de ellos. Esto es así porque, sin duda, ofrecen muchas ventajas. Un desarrollador informático con cierta experiencia podría desarrollar uno en Ethereum en apenas unos días, y de esto las empresas se han dado cuenta, así como de las posibilidades que les proporciona.

Si una empresa ha desarrollado un token y lo vende, dispone de capital por adelantado para financiar nuevos proyectos. Entramos aquí en una realidad ciertamente interesante relacionada con la financiación en el ámbito empresarial: es lo que se conoce como los *token crowd sales* o *Initial Coin Offering* (ICO), otra de las aportaciones revolucionarias que trae la criptoeconomía. El nombre no ha sido escogido al azar, es un guiño a los famosos IPO —*Initial Public Offering*—o salida a bolsa de la época del dot.com, pero con otras características que veremos más adelante.

LOS CRYPTOKITTIES, LA APLICACIÓN DE MÁS ÉXITO DE ETHEREUM

Con permiso de las ICO, la que por ahora se ha coronado como la mayor aplicación de Ethereum y que casi colapsa la red es la conocida como CryptoKitties —o criptogatitos—, una aplicación para

coleccionar, comprar e intercambiar gatitos virtuales en la red de Ethereum de una forma totalmente distribuida. Lo que fue lanzado como un experimento por la empresa de desarrollo Axiom Zen en el mes de octubre de 2017, se convirtió de la noche a la mañana en el éxito más importante hasta el momento de Ethereum.

En el juego los usuarios pueden, como hemos dicho, criar, coleccionar, comprar y vender gatitos digitales, así como relacionarse con la comunidad de propietarios de estos. Cada criptogatito es único, su propiedad está validada por un contrato inteligente en la blockchain de Ethereum, y su valor depende del mercado. Cada gatito tiene un aspecto totalmente diferente, dependiendo de genes inmutables almacenados en el contrato inteligente. Es, en cierto modo, parecido al juego Pokémon, pero en la blockchain.

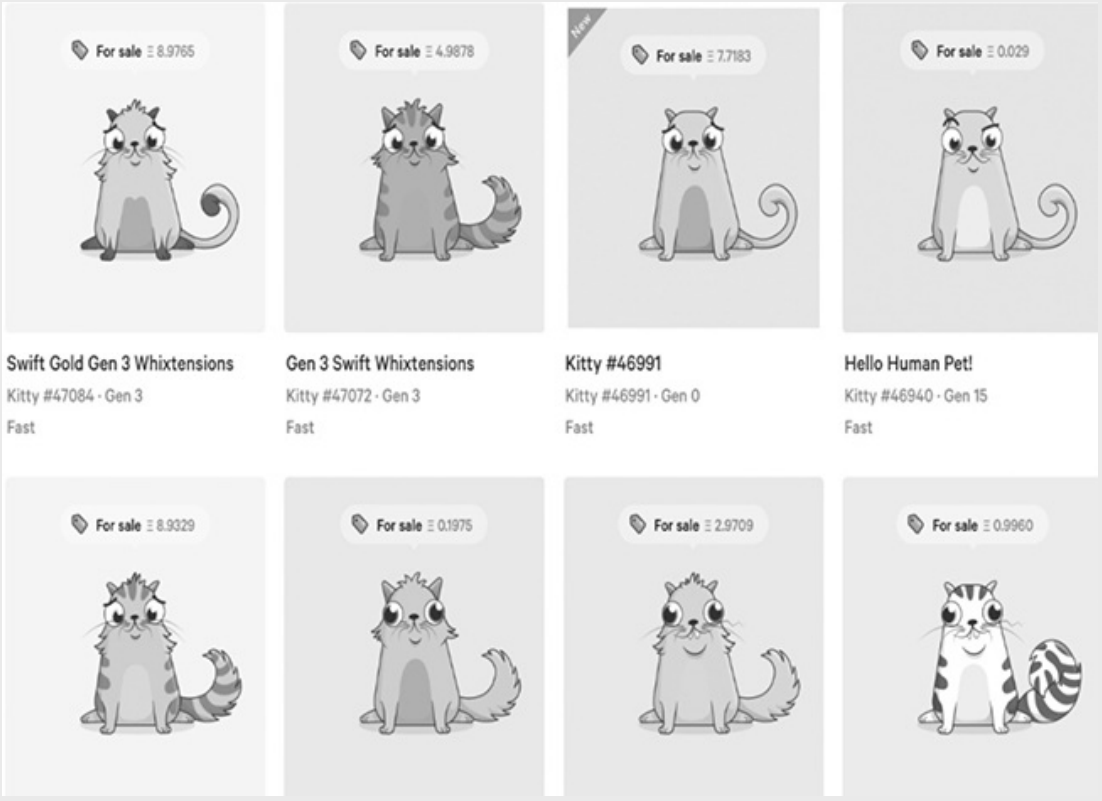
Es una aplicación muy sencilla y para muchos fue la primera vez que utilizaron una aplicación distribuida desarrollada en Ethereum. La aplicación es básicamente un interfaz que permite al navegador interaccionar con los contratos inteligentes de la red de Ethereum que gobiernan las propiedades de los gatos virtuales, así como interaccionar con tu monedero de criptomonedas para poder comprarlos o venderlos.

En diciembre de 2017 la aplicación se había viralizado, y algunos de los gatitos virtuales ya costaban decenas de miles de dólares pagados en ethers, la criptomoneda de la red, y su elevado uso llegó a disparar las transacciones en Ethereum unas seis veces más que en el mes anterior, batiendo el récord de transacciones procesadas hasta el momento, pero llegando también a casi colapsar la red y acumular muchísimas transacciones no procesadas.

Las consecuencias no esperadas de estos problemas de escalabilidad es que la comunidad de Ethereum y los desarrolladores de los diferentes proyectos involucrados en el juego, crearon rápidamente un equipo de trabajo y de manera colaborativa empezaron a formular mejoras que se podían implementar en la red de Ethereum y sus aplicaciones para mitigar el colapso actual. Esto sirvió también para preparar un

roadmap sobre mejoras para el escalado de Ethereum que puede ser muy beneficioso para el futuro de esta blockchain.

Además, este juego, por muy banal que sea, ha demostrado a mucha gente el potencial para crear y tokenizar activos en la red de Ethereum y comercializar de forma segura y descentralizada con ellos. De manera que, quién sabe, quizás en el futuro el éxito de Ethereum habrá que agradecérselo a estos bonitos gatitos virtuales.



NUEVAS ALTERNATIVAS PARA FINANCIAR Y MONETIZAR

Todo lo expuesto en relación con los tokens y la digitalización de la propiedad nos está conduciendo a una de las ideas más poderosas que incorpora la revolución de la blockchain: el enorme potencial que ofrece para encontrar formas innovadoras de financiación de nuevos proyectos y de proveer liquidez a inversores financieros.

Vitalik Buterin predicó con el ejemplo, puesto que en la propia creación de Ethereum demostró ya lo que significa una ICO, pues fue el método de financiación de la plataforma. Se realizó así la primera ICO de la historia: la creación de la moneda ether y su preventa pública a través de *crowdfunding*. Irónicamente en el caso de quien creaba una plataforma nueva porque no había sido aceptada su idea en la comunidad Bitcoin, Buterin y la Ethereum Foundation aceptaron el pago con bitcoins, y llegó finalmente a recaudar 14 millones de dólares al precio del bitcoin de aquella época, con los que financió el desarrollo de la plataforma Ethereum.

A partir de ese momento, esta forma de financiación a través de ICO y con el empleo de tokens se convierte en una alternativa de financiación cada vez más tenida en cuenta, y resulta especialmente atractiva a la hora de financiar a las start-ups. Durante el año 2017 esta fórmula ha explotado en tamaño hasta alcanzar los 5000 millones de dólares, y ha superado al tradicional capital riesgo como la forma de financiación más usada por las empresas de blockchain. En este contexto, se convierte, además, en una vía para que los inversores obtengan más rápidamente liquidez, que suele ser uno de los inconvenientes a la hora de financiar este tipo de ideas empresariales innovadoras en fase de lanzamiento.

Como sabemos, una start-up es una empresa emergente con una idea de producto innovadora, generalmente vinculada a las nuevas tecnologías y la digitalización, y que necesita capital para poder desarrollarla. El método tradicional para que consigan financiación pasa por acudir a empresas de capital riesgo, las cuales les invierten dinero a cambio de una parte de las acciones o derechos sobre la nueva empresa. Como su propio nombre indica, estas entidades asumen un riesgo en dependencia del éxito futuro de la start-up, de manera que si a esta le va mal, puede perder toda o parte de la inversión. En cambio, si acierta con su idea innovadora, su revalorización suele ser muy alta.

Por otro lado, obtener liquidez de esta inversión no es algo inmediato, pues requiere que la start-up crezca lo suficiente para poder salir a bolsa y vender acciones, o que haya alguien que decida comprarla. Hasta ese momento, el inversor tiene su capital invertido inmovilizado, no dispone de ninguna liquidez derivada del mismo.

Este vendría a ser el método tradicional de financiación de las start-ups, que trae algún inconveniente no solo a los inversores que arriesgan y tardan en tener liquidez, sino también a las propias start-ups, ya que, aunque obtengan financiación, no dejan de vender parte de su empresa y a menudo quedan un

tanto cautivas de las condiciones impuestas por las empresas de capital riesgo y en general tienen acceso a capital muy limitado.

Las ICO permiten cambiar todo esto. Como hemos comentado, su nomenclatura ya nos recuerda en inglés a la utilizada en la salida a bolsa de las empresas —IPO: *Initial Public Offering*—, y efectivamente existe un paralelismo, aunque con la innovación de producirse en un entorno digital y basado en las criptodivisas y la tecnología de la blockchain.

Aquí lo que emiten las empresas son los tokens, a los que asignan algún tipo de valor o uso para venderlos en operaciones gobernadas por *smart contracts* antes de que la empresa se haya desarrollado y tengan una aplicación práctica. Con ello, están financiando un proyecto que, una vez lanzado y crecido, puesto que la emisión de tokens está vinculada específicamente a una política monetaria que es inmutable, permitirá su revalorización y el beneficio de quienes invirtieron. Por supuesto, el inversor apuesta porque ese negocio del que adquiere tokens va a crecer y estos se van a revalorizar, y que el token está bien diseñado.

Recurramos a los ejemplos citados de los casinos o los festivales de música. Pongamos que uno quiere crear un festival, y en vez de pedir un préstamo convencional lo que hace es prevender el dinero propio del festival que va a emitir y que se va a convertir en el único medio de pago válido dentro del recinto. Con lo que las personas interesadas en el festival le vayan aportando con antelación a cambio de esa «moneda del festival», de esos tokens, el promotor va a poder ir financiando el mismo.

Quienes hayan comprado esos tokens, por supuesto disponen de ellos para consumir dentro del festival y, teóricamente también tendrían la oportunidad de revenderlos obteniendo un beneficio. En la práctica esto no es posible en este contexto —lo mismo ocurre en el de los casinos—, puesto que la paridad está fijada y la cantidad de tokens no está limitada y, en consecuencia, no cabe la revalorización de los mismos.

Pero imaginemos que efectivamente la emisión total de tokens sí estuviera limitada a un número fijo de, pongamos, un millón de tokens vendidos inicialmente a un euro por cada uno en una ICO. En ese caso, a medida que el festival crezca y vaya captando un mayor interés en el público, crecerá también la demanda por asistir y por tener tokens con los que poder consumir allí. En algún momento, la necesidad de consumo de las personas que quieran ir al festival estará por encima del millón de euros en tokens que circulan por el mercado y, por lo tanto, el valor del token subirá como reflejo de este aumento

de demanda. En este caso, indudablemente se revalorizaría el valor del token, y quienes cuentan con ellos se encontrarían con una demanda grande que les permitiría obtener ganancias.

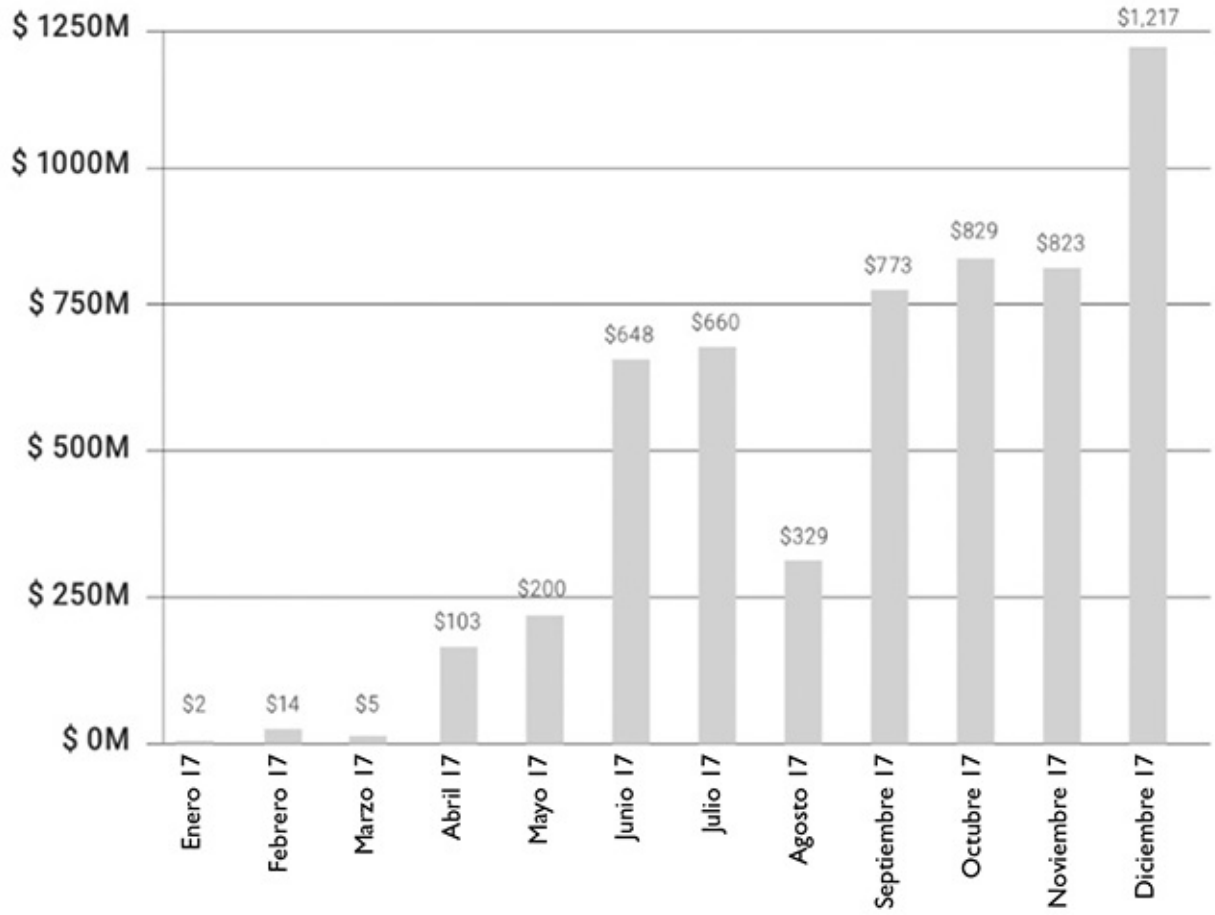
El token es, por lo tanto, una utilidad futura en un negocio, pero vendido al público antes de que esa utilidad sea real. Habrá quienes compren tokens porque quieran usar el servicio —quienes quieran asistir al festival de música, ver los conciertos, consumir algo allí—, pero también quienes lo hagan por motivos especulativos —confían en el éxito del festival y cuando tengan la oportunidad revenderán sus tokens a quienes deseen asistir al festival, que ya no los podrán adquirir porque no se emiten más—.

Esto es sintéticamente lo que es una ICO, y aunque por primera vez se empleó para financiar la criptomoneda de Ethereum, como vemos su aplicabilidad es mucho más amplia, y no cabe dudar de sus enormes ventajas, tanto para quienes buscan financiación como para inversores, puesto que suelen ofrecer una alta rentabilidad y, sobre todo, una liquidez temprana que no acostumbra a ser habitual en este tipo de negocios.

Lo cierto es que al principio las ICO no fueron muy populares cuando surgieron en 2014, y realmente no fue hasta 2017 cuando experimentaron un *boom* espectacular. Una de las primeras fue la que comentaba en la Introducción que llevó a cabo mi amigo Brendan Eich, uno de los fundadores de Mozilla, la empresa que revolucionó Internet con su navegador Firefox, quien lanzó la ICO para financiar su nuevo proyecto Brave, un navegador de Internet tipo Internet Explorer de Microsoft o Chrome de Google, pero con una peculiaridad muy importante: en el navegador Brave lleva incorporado de forma nativa la funcionalidad de bloquear todo tipo de anuncios y publicidad en las páginas web que visitas.

A partir de este momento se desata una fiebre por las ICO que llegan a adquirir tamaños desorbitados, muy por encima de los que se manejaban antes en las start-ups. Hay que reconocer que las ICO han tenido los retornos financieros más altos de la historia. Un reciente estudio de Mangrove VC decía que si alguien hubiera invertido la misma cantidad en todas las ICO que ha habido desde que nacieron hasta finales de 2017 —eso incluiría las que triunfaron y las que no—, en un periodo de tiempo mínimo habría obtenido un retorno de 12,5 veces el capital invertido.

En el siguiente gráfico podemos ver las cantidades totales en dólares que se han conseguido como financiación a través de ICO durante el año 2017.



Cantidad de dinero invertido en ICO (en dólares y mensualmente) durante el año 2017.

Con todo, también se ha producido en relación con las ICO algún contratiempo que ha socavado la confianza en la plataforma Ethereum. En 2016 se puso en funcionamiento una ICO con el objeto de recaudar 150 millones de dólares para financiar una DAO —*Descentralized Autonomous Organization*—, esto es, organizaciones autónomas descentralizadas que buscan establecer plataformas donde cada uno de sus miembros pueda desarrollar y ejecutar aplicaciones que les permitan beneficiarse tanto de forma individual como colectiva. Es algo que se está extendiendo mucho en el entorno blockchain.

En este caso se pretendía crear una DAO que invirtiera en otros proyectos descentralizados a modo de empresa de capital riesgo, pero en la que, como organización descentralizada y sin *management*, las decisiones sobre qué financiar y otras se tomarían por consenso entre quienes participaran antes en el

proceso de *crowdfunding*. La ICO se llevó a cabo con el pertinente contrato inteligente, pero se produjo un error en su programación que podía permitir que alguien se aprovechara del fallo y fuera capaz de trasladar una parte de las criptomonedas de un monedero a otro.

Recordemos que en la tecnología blockchain estas operaciones son irreversibles, por lo que un error de este tipo supone un riesgo enorme para la plataforma y la confianza que ofrece. No se trató de un problema de seguridad o de un hackeo, sino de un error de programación, pero supuso un gran reto para Ethereum a la hora de afrontar una solución. Se optó por una bifurcación como única salida posible, dando como resultado dos cadenas de bloques, Ethereum y Ethereum Classic, que continuaba con la programación de la blockchain inicial. Ethereum es, ya lo hemos dicho, la segunda criptomoneda en importancia, pero Ethereum Classic también se ha mantenido entre las más destacadas.

A pesar de este caso concreto, las ICO siguen despertando unas expectativas enormes. Se están invirtiendo miles de millones en tokens que las empresas generan y, algo interesante, están desplazando al capital riesgo tradicional en este sector del mercado. Ahora mismo, las empresas que emiten tokens no tienen la necesidad de acudir a empresas de capital riesgo para financiarse, porque han encontrado un modo de autofinanciarse.

Por supuesto que esto está generando también cierto abuso, y salen al mercado ICO improcedentes que se saltan la regulación, y hay fraudes de diverso tipo. Como todo mercado en ebullición, atrae también a los malos actores en busca de dinero fácil. Las ICO distan todavía bastante de ser un medio de financiación perfecto, les falta una regulación adecuada y no son válidas para todos los casos ni empresas. Sin embargo, no se puede poner en duda su capacidad transformadora para el futuro de los mercados financieros.

Hay quien habla igualmente de burbuja, pero si lo ponemos en contexto con otras formas de financiación, en realidad siguen todavía representando muy poco: menos de un 10 % de lo que se recauda por *crowdfunding* corresponde a ICO, y aún es más insignificante si se compara con el capital riesgo, ya que las ICO no representan ni el 1 % del dinero invertido en capital riesgo durante el año 2017.

El margen de crecimiento es muy grande, y lo cierto es que están proporcionando en estos momentos los mejores retornos que hay para los inversores. Como es obvio, no es sostenible el nivel actual de retorno, pero incluso asumiendo que van a bajar bastante, siguen garantizando una gran

rentabilidad. Y es especialmente, lo repetimos, en su capacidad para aportar liquidez donde reside su gran valor.

TELEGRAM, LA MADRE DE TODOS LAS ICO

Si hay una ICO que parece que despuntará en 2018 es la de la aplicación de mensajería Telegram. Lo sorprendente de esta ICO —de la que todo el mundo habla, y sobre la que los inversores andan desesperados por intentar entrar en ella— es que en realidad todavía no se ha anunciado de manera oficial. Por la documentación ya filtrada de forma extremadamente amplia, se puede leer que los planes de Telegram son construir una nueva plataforma de blockchain denominada TON —*Telegram Open Network*— que rete el hasta ahora liderazgo de Ethereum y se posicione como la plataforma de nueva generación. Esta promete incorporar los avances más recientes —y algunos sin desarrollar— de tecnología blockchain, de forma que permitan una red más sostenible eliminando el minado tradicional, transacciones inmediatas y con alto volumen y una alta seguridad, a pesar de su naturaleza no cien por cien descentralizada. Telegram también ha anunciado otros servicios como parte de su blockchain TON, como los pagos o el almacenamiento en la nube más allá de los contratos inteligentes que, obviamente, también soportará.

Y es para financiar este proyecto que Telegram está conduciendo, de momento de forma privada, la que podemos denominar como la madre de todas las ICO, en la cual se estima que puede llegar a recaudar más de 1500 millones de dólares.

Es importante entender que Telegram es una aplicación de mensajería que cuenta con cerca de 200 millones de usuarios en el mundo, y que es la aplicación de mensajería usada de forma mayoritaria por la comunidad de cripto y blockchain, gracias a su adopción temprana de la encriptación de los mensajes y su sencillez a la hora de crear grupos con miles de usuarios para discutir diferentes temas. No hay ICO que no tenga su grupo de Telegram donde se discuta el proyecto y la inversión.

A la hora de publicar este libro el tema está candente sobre la mesa, y cuando tengas ante ti estas páginas quizás dispongas ya de más información sobre cómo va el proceso. Por ahora, las dudas de la comunidad sobre la capacidad tecnológica de Telegram para llevar a cabo un proyecto tan ambicioso, y las reacciones negativas a la cantidad de dinero que pretenden recaudar —que no parece que sea necesario para un proyecto de estas características—, no han sido un obstáculo para que los inversores acudan en masa al proyecto, y todo parece indicar que se convertirá en la ICO más grande del mundo durante el año 2018.

LA REVOLUCIÓN DE LA LIQUIDEZ

Podemos concluir con la idea de que uno de los aspectos más importantes que ha traído consigo la segunda generación de blockchain es su capacidad de proporcionar liquidez a los mercados financieros a través de los tokens. Si se confía en que el bitcoin va a transformar lo que es el dinero en sí, de las ICO cabe esperar que transformen el mercado de productos financieros mediante la «tokenización» de los activos y la provisión de liquidez.

Ese es el siguiente gran paso en este proceso evolutivo: la «tokenización de las cosas». Los token nos sirven para consumir en nuestro festival de música o dentro de un casino, pero también pueden usarse para representar un tipo de interés económico dentro del negocio que admite muy diversas formas. Por ejemplo, a un token se le puede conceder el valor del 10 % de todos los consumos que se realicen en *merchandising* dentro del festival.

En caso de que un negocio prospere, el token garantiza un retorno económico líquido. No es muy diferente a comprar acciones de una empresa en bolsa: el token habitualmente no concede todos los derechos que poseen los accionistas, pero sí los derechos económicos que queden fijados mediante los contratos inteligentes pertinentes. Los *smart contracts* garantizarán que, de forma automática, el dinero llegue a los poseedores de tokens en función de los derechos, plazos y proporciones que les correspondan.

Gracias a estos contratos inteligentes la gestión de los derechos económicos y los retornos que se tienen que hacer para los inversores en tokens de forma

periódica, se pueden realizar de manera extremadamente eficiente y con un coste muy bajo. En el entorno financiero actual sería imposible hacerlo sin una complejidad y un coste altísimos.

Por eso decíamos al principio que Bitcoin ha digitalizado el dinero, mientras que Ethereum ha digitalizado la propiedad, puesto que tokenizar un activo es exactamente eso, digitalizar la propiedad.

Cuando tokenizamos —en castellano podríamos decir titularizamos o securitizamos— un activo le estamos asignando un token mediante un *smart contract* que te otorga los mismos derechos económicos que el activo original, y ofrece, además, una enorme escalabilidad. Pero lo más importante: libera liquidez, algo fundamental en la industria financiera.

Esto nos sirve para un piso, un hotel, una obra de arte… El token proporciona fracciones de propiedad, y es particularmente válido en el caso de activos muy costosos. Si un cuadro de Picasso vale 10 millones de euros, muy pocas personas van a poder comprarlo, pero si se generan tokens y a cada una de ellas se le da el valor de una fracción del precio total, se incrementan las posibilidades de venderlo. Hay mucha gente que podría tener interés en invertir en un cuadro de Picasso, y de esta manera sería accesible, mientras que no se daría el caso si se tuviera que comprar el cuadro entero. Y esto mismo sirve para un hotel de lujo o un castillo si se quiere.

Estamos ante algo mucho más valioso y revolucionario de lo que parece, ya que aporta liquidez en los mercados al facilitar la venta de activos que son precisamente difíciles de transformar en líquido. Al final es un problema de precio. Tokenizar es dar propiedad fraccional y liberar liquidez, y esto representa toda una revolución financiera, ya que en el mundo se estima que hay alrededor de 500 billones de dólares en activos financieros con problemas para ser convertidos en dinero líquido —aproximadamente la mitad corresponde al sector inmobiliario—. Además, su valor podría elevarse entre un 20 y un 30 % gracias a ese proceso de tokenización que libera liquidez. Un montón de inversores van a poder invertir en lo que antes no podían, y en consecuencia subirá el precio del activo subyacente.

El universo que se abre ante nosotros de cara al futuro es sencillamente espectacular y nos queda mucho por ver con respecto a su enorme potencial.

TERCERA PARTE
EL FUTURO DE LA CRIPTOECONOMÍA

7
ALGUNOS MITOS Y MUCHAS EXPECTATIVAS

EL AÑO NETSCAPE DE LA CRIPTOECONOMÍA

El principal cometido con que afrontaba este libro era ser capaz de ofrecer a un público amplio, no necesariamente experto en tecnología ni familiarizado con el entorno financiero, un acercamiento conceptual e histórico al universo cripto, en un momento en el que está dando tanto que hablar y llegados a un punto que yo considero decisivo dentro de su evolución y desarrollo.

Esencialmente, ese ha sido el camino que hemos recorrido hasta el momento en las páginas precedentes: nos hemos dedicado a observar el contexto en el que ha irrumpido el dinero digital, aclarar conceptos, comprender la tecnología que subyace, apuntar las implicaciones que conlleva… Hablamos de un periodo de tiempo de apenas una década desde que el bitcoin vio la luz, pero no cabe duda de que ha sido intenso, que muchas cosas han cambiado ya, y que nos ha aportado unos cuantos elementos ciertamente innovadores para el debate.

Pero no me parece suficiente limitarme a una mera explicación divulgativa que repasa un pasado reciente y aclara conceptos. Manejamos algo que, tal y como me encargaba de proclamar desde la Introducción, tiene un potencial revolucionario, de manera que me exige —nos exige— que extienda la mirada, que la extendamos todos, no solo hacia atrás, también hacia adelante, hacia lo que el futuro puede traernos en este terreno con tantas posibilidades. Las expectativas son altas, sin duda.

Esta mirada hacia el futuro cobra, además, especial alcance en un momento en el que tenemos muy reciente el haber cruzado un punto de inflexión especialmente significativo: el vivido en el pasado 2017, el año Netscape de la criptoeconomía. Recordarás que ya hemos empleado antes la expresión en estas páginas.

Como quizás ya sepas, Netscape fue el primer navegador comercial que hubo en Internet, mucho antes de los usados ahora como Firefox de Mozilla, Safari de Apple o Chrome de Google. Apareció en 1995, y con él se comenzó a popularizar para la gente la idea de poder conectarse y navegar por las páginas de esa red llamada Internet, accediendo a distintos tipos de información. En realidad, el concepto de Internet existía mucho tiempo antes, desde 1981, año en el que se había llegado ya a formular el primer protocolo, pero no fue hasta 1995 cuando todo eso llegara a asentarse y, algo importante, se percibiera como una realidad comercial y no solo como una fantasía de informáticos o ingenieros.

Además, ese mismo año 1995 Netscape llevó a cabo también una IPO —u OPV, Oferta Pública de Venta, en español— con la que comenzaba a cotizar en bolsa, otro rasgo distintivo que marca ese momento como clave en la evolución de Internet. Lo cierto es que, en la práctica, el grado de penetración de Internet entre la población todavía no alcanzaba siquiera el 1 %, pero a través de la visibilidad de Netscape, su existencia, su realidad, se había popularizado, había salido a la luz y se encontraba ya a la vista de la mayor parte de la población. Y eso es básicamente lo que se entiende como el año Netscape: la popularización global de Internet gracias a la irrupción de este navegador comercial y a su exitosa salida a bolsa.

En 2017 podemos decir que sucedió algo similar con respecto a la criptoeconomía. Como bien sabemos, el bitcoin nació unos cuantos años antes, pero fue en este año cuando el «fenómeno popular» explotó, el año en el que las ICO experimentaron su *boom* particular, produciéndose el primer impacto de ICO exitosas. Es el año, como hemos visto, en que la cotización del bitcoin se disparó por encima de los 10 000 dólares —de hecho, por un breve tiempo, llegó a cotizar hasta los 20 000 dólares— y cruzó la barrera de una capitalización de mercado por encima de 100 000 millones de dólares, arrastrando también un gran dinamismo en el mercado de otras criptodivisas.

Otro paralelismo con lo que sucedió en 1995 con respecto a Internet es que, en realidad, solo unos pocos manejaban en la práctica criptomonedas o tokens —menos de 50 millones de personas en todo el mundo, es decir, ni el 1 % de la población—, pero el ruido mediático ya se había producido, con el añadido de que ahora ya existen Internet y las redes sociales —que al fin y al cabo es lo que estaba irrumpiendo entonces—, por lo que este ruido mediático se amplifica hoy en día muchísimo más.

De manera que, aunque realmente el nivel de penetración siga siendo muy bajo, no podemos poner en duda que lo cripto, el bitcoin, los tokens, las ICO,

etc., se han popularizado, y como ocurría en 1995 con Internet, solo estamos viendo la punta del iceberg. La realidad es que hoy todo el mundo habla de cripto, bitcoin o parece que todas las start-ups quieren hacer una ICO, pero en verdad es que pocos los emplean o entienden demasiado bien. Lo mismo pasaba en 1995 después de la salida a bolsa de Netscape, que todos hablaban de Internet, pero casi nadie la usaba. Todo esto va a terminar explotando en cuestión de uso, aplicaciones reales y reconocimiento en los próximos años, aunque aún estamos arrancando y nos movemos en un entorno muy incipiente y muy poco maduro.

Siguiendo con los paralelismos entre uno y otro de los años Netscape, también podemos prever que, de hecho, quién sabe, es posible que el bitcoin se quede finalmente reducido a una función de oro digital y no consiga dar el salto a convertirse en una auténtica moneda, o pierda todo su valor porque él mismo se desplace a otra criptomoneda con mejores propiedades y tecnología. Sería similar a lo que le sucedió a la propia Netscape, o a Lycos/Terra, o Altavista, y a otras empresas pioneras en su día en Internet, que luego fueron desplazadas por nuevas propuestas como Google y Facebook —que son las que finalmente se han impuesto hoy—. Por eso, muchos creen que en el caso de las criptomonedas tampoco habrán de ser las actuales las que triunfen, sino las que están por llegar y sean capaces de solucionar los problemas e inconvenientes que existen, o de dar respuesta a los nuevos retos que han de surgir.

Considero que acabamos de cruzar una frontera y que debemos preguntarnos en qué punto estamos y cuáles son las perspectivas de futuro. Por eso, me parece fundamental que dediquemos esta última parte del libro a proyectar nuestra mirada hacia lo que está por venir en torno a la criptoeconomía y que en buena medida está sucediendo ya porque en este mundo todo resulta extremadamente acelerado. Debemos identificar las posibilidades que se abren ante nosotros con esta tecnología, descubrir su potencial y perspectivas, atender a su evolución y a los retos que deben afrontarse, y ser capaces de manejar las expectativas de un modo realista.

Ya sabemos que hay posturas enfrentadas, desde aquellos que observan esto con un fervor casi religioso y plena confianza en el elemento revolucionario de la criptoeconomía, hasta quienes no dejan de apuntar constantemente y de forma casi apocalíptica riesgos y problemas en relación con la misma. El debate está servido y la polémica en boca de todo el mundo.

Por eso mismo es tan valioso que analicemos con un mínimo de calma lo que puede estar por venir. Y quiero comenzar, puesto que es conocida mi postura

como la de alguien que cree que en efecto nos encontramos ante algo disruptivo, por responder, ahora que se habla tanto de ello, a las múltiples críticas que se le hacen al universo cripto, lo cual ha terminado levantando ciertos mitos en torno al mismo que no siempre están justificados. Luego ya pasaremos a lo largo de sucesivos apartados a plantearnos los principales elementos que afectan al futuro de la criptoeconomía: retos pendientes, las nuevas generaciones de criptomonedas y blockchains, y los impactos previsibles en los ámbitos financieros, económicos y empresariales.

DESMONTANDO MITOS

El haber vivido recientemente, como acabamos de explicar, ese año Netscape de la criptoeconomía, trae consigo una serie de consecuencias que estamos experimentando ahora mismo.

Acabamos de ver la irrupción popular de un fenómeno que, como todo lo nuevo, da mucho que hablar y alcanza una enorme difusión, especialmente en la era digital, pero que también debe enfrentarse a la muy humana resistencia al cambio. Lo nuevo provoca curiosidad en la mayoría y entusiasmo en unos cuantos, pero también miedos y suspicacias en no pocos, sobre todo cuando de fondo hay aspectos técnicos de carácter tecnológico y financiero un tanto complejos que no son sencillos de comprender —de ahí la importancia otorgada a la parte histórica y conceptual—. Como consecuencia de ello, se han elevado también muchas voces críticas con la criptoeconomía, con opiniones a menudo exageradas o no del todo justificadas, que han dado lugar a una serie de mitos que considero que merece la pena que sean respondidos.

¿SON EL BITCOIN O LAS CRIPTOMONEDAS UN ESQUEMA PONZI?

Una de las críticas habituales de gente tan reconocida como el Premio Nobel Paul Krugman o Yves Mersch, uno de los ejecutivos más importantes del Banco Central Europeo, sobre el bitcoin o las criptomonedas es que todo esto no es sino un esquema piramidal, lo que se conoce como un esquema Ponzi. Pero ¿lo es de verdad?

Veamos primero qué es exactamente un esquema Ponzi para entender si es aplicable al bitcoin y las criptomonedas en general.

Aunque esquemas piramidales siempre han existido, el nombre de esquema Ponzi se refiere a la estafa inventada por Carlo Ponzi, un italiano emigrante en Estados Unidos durante principios del siglo XX. En estos esquemas, típicamente el promotor —Carlo Ponzi en este caso—, promete a los inversores retornos desorbitados por un activo —en su caso unos cupones de respuesta de correos que, según él, se podían traer de Italia y vender más caros en Estados Unidos—, cuando en realidad esos retornos no existen, sino que básicamente se pagan a los inversores existentes con el dinero de los inversores nuevos, y así de forma continuada —de ahí también el concepto de esquema piramidal—.

Otro caso reciente ha sido el de Bernie Madoff, en Estados Unidos, que llevó a cabo el fraude piramidal más grande de la historia, defraudando más de 60 000 millones de dólares de cerca de 5000 inversores.

De modo que aquí podemos ver que, en un esquema Ponzi o piramidal, tienes un promotor central que es el que promete retornos y continúa incentivando a nuevos inversores para entrar, y así poder pagar esos «retornos» a los anteriores.

Nada de eso existe en general en el bitcoin o las criptomonedas. Cuando la gente compra bitcoins no hay ningún tipo de retorno garantizado que sea prometido por una entidad central. Bitcoin y las criptomonedas son activos económicos descentralizados y con políticas monetarias completamente transparentes e inmutables. Pueden ser malas inversiones si no acaban triunfando, pero no son para nada un esquema Ponzi, y referirse a ellos con este término solo implica desconocimiento de su significado.

Sobre el bitcoin y, por extensión, sobre otras criptomonedas y, en general, sobre el dinero digital, incluso la criptoeconomía en su conjunto, se vienen escuchando en la opinión pública críticas reiteradas sobre ciertos aspectos tales como que no tiene un valor intrínseco ni nada que lo sustente por debajo; sobre sus problemas de seguridad; acerca de su vinculación a actividades ilegales; en

relación con el elevado coste energético que implica su funcionamiento a través de unos procesos de minería que exigen equipos muy sofisticados; o, muy especialmente, sobre que se trata de un fenómeno «de moda» fruto de una fuerte especulación que está dando lugar a una burbuja.

Es comprensible que, en un momento tan delicado, en un terreno tan inmaduro y en esta era digital tan proclive al ruido mediático se cuestione algo que irrumpe de forma tan potente y con afán revolucionario, pero suele ser habitual que las críticas, aunque a menudo partan de algún fundamento, también se magnifiquen demasiado, e incluso den lugar a mitos injustificados, como puede estar ocurriendo en este caso. Es importante distinguir el ruido de las nueces.

Por eso quisiera comentar brevemente algo al respecto de todos esos aspectos críticos que salen constantemente a colación, porque además así vamos a comprender mucho mejor los puntos débiles y fuertes del universo cripto, los retos que hay que afrontar y su potencial futuro.

¿No tiene valor intrínseco?

Sobre este aspecto ya hablamos cuando en nuestra breve historia del dinero comprobamos que el fiduciario también dejó de sustentarse sobre el patrón oro y, por lo tanto, tampoco el dólar o el euro tienen un valor intrínseco ni están sustentados por nada debajo que no sea la confianza que los usuarios le otorguemos a esas monedas y el acuerdo común.

Lo mismo cabe decir del valor que haya de concedérsele al bitcoin u otras criptomonedas, por lo que no cabe distinción en este sentido con respecto a las que emiten nuestros bancos centrales. Es decir, si el bitcoin u otra criptomoneda ganan aceptación y confianza, el que no tengan valor intrínseco no supone ningún tipo de problema para su adopción y uso futuro.

¿Relacionada con actividades ilegales?

Aquí no podemos menos que recordar el dañino efecto que produjo aquella polémica de Silk Road, así como los múltiples hackeos que ha habido en la historia reciente de las criptomonedas.

Como decíamos páginas atrás, esa imagen negativa del bitcoin como la moneda empleada en negocios ilegales, o como vía para blanquear dinero, le sigue persiguiendo, y todavía sigue pesando en la mentalidad de la gente. Pero como también ya se ha explicado antes, ese en el fondo es el problema

irresoluble del dinero en metálico, que es el medio de pago que sigue estando más extendido para las transacciones ilegales. ¿Prohibimos el dinero en metálico? No tiene mucho sentido: es un medio que se emplea mucho para el blanqueo y las actividades ilícitas, pero también para comprar el pan. Recordemos que el dinero digital es su equivalente, en lo bueno y en lo no tan - bueno.

En cualquier caso, el digital es más transparente que el dinero en metálico, ya que cada transacción, como hemos dicho, deja traza. Es verdad que el dinero es anónimo en la mayoría de los casos, pero se le puede seguir la pista. Así, por ejemplo, si alguien ha tenido que pagar en bitcoins algún tipo de extorsión, o si se han robado los bitcoins de un monedero accediendo a sus claves privadas, esos se pueden tracear en la blockchain de Bitcoin y, por lo tanto, señalarlos como contaminados para futuros usos, ya que han sido obtenidos de forma ilegal.

FACEBOOK PROHÍBE LOS ANUNCIOS SOBRE CRIPTOMONEDAS E ICO

En febrero de 2018, Facebook anunciaba por sorpresa que había cambiado la política de sus anuncios y que prohibía toda publicidad de criptomonedas —incluyendo el bitcoin— e ICO. En su nota de prensa se refería a los mismos como «productos financieros y servicios frecuentemente asociados con prácticas promocionales engañosas».

Facebook viene a decir que considera que todos los anuncios de criptomonedas o ICO son generalmente engañosos y que buscan confundir al usuario. La prohibición se extiende también a Instagram y a su plataforma para anuncios en páginas de terceros Facebook Audience Network. Lo cierto es que la fiebre de las ICO y las criptomonedas ha atraído todo tipo de malos actores que se intentan aprovechar del desconocimiento del público en general de estos productos financieros para atraer sus inversiones.

Sin embargo, hay que decir bien claro que también hay muchos servicios de compra y venta de criptomonedas y muchas ICO que son completamente legítimos y que, por lo tanto, la medida de Facebook parece en principio exagerada, ya que también penaliza a todos los servicios honestos que solo buscan una audiencia sin intentar engañar

a nadie. La alternativa más adecuada parece que hubiera sido simplemente filtrar los anuncios para dejar pasar unos y no otros, y publicar una guía de buenas prácticas que las empresas anunciantes de estos productos estuvieran obligadas a cumplir. Claro que eso hubiese significado que Facebook hubiera tenido que dedicar recursos para implementar este sistema, de manera que lo que parece es que han optado por el método más sencillo de, simplemente, bloquearlos todos.

Sin embargo, esto choca bastante con el anuncio reciente que realizaba el propio Mark Zuckerberg según el cual se imponía como desafío para 2018 —ya es tradición desde el año 2009 que Mark Zuckerberg anuncie y realice retos anuales, como esos años que aprendió chino mandarín, leyó veinticinco libros, visitó todos los estados de Estados Unidos o construyó un asistente virtual basado en inteligencia artificial como el de las películas de *Iron Man* para su propia casa— aprender más sobre las criptomonedas y la encriptación.

Zuckerberg se planteaba descubrir el potencial del universo cripto para llegar así a reducir el poder de los sistemas centralizados —como el que ha llegado a acumular de manera imponente el propio Facebook, lo cual es admitido obviamente por su mismo creador— y descentralizarlos. Al fin y al cabo esto era una promesa de los inicios de Internet que no ha llegado a cumplirse, aunque los entusiastas de las criptomonedas y de blockchain creen que esta vez será una realidad gracias a estas nuevas tecnologías.

¿Falta de seguridad?

La cuestión de la seguridad del bitcoin y del dinero digital, en general, exige una explicación más amplia, y merece la pena extenderse un poco porque esta seguridad —o falta de ella— está siendo permanentemente sometida a debate.

En este caso, la herencia dejada por lo ocurrido con MtGox también pesa mucho. Parece que se transmitió una sensación de que la criptomoneda o la tecnología de la blockchain podía ser fácilmente hackeada.

Sin embargo, es importante entender que ninguno de estos hackeos de *exchanges* como MtGox —que de hecho no han sido ni mucho menos el único:

por ejemplo, Bitfinex, que fue la *exchange* que la reemplazó como la más grande del mundo, perdió 72 millones de dólares en bitcoins en 2016— han sido debidos a fallos de seguridad del bitcoin.

Conviene recordar que antes de cualquier problema de hackeo de *exchanges*, en agosto del año 2010, ya se detectó una primera gran vulnerabilidad en el protocolo Bitcoin. Hasta ese momento las transacciones no eran verificadas antes de ser incluidas en la cadena de bloques, lo que podía permitir a los usuarios superar las restricciones de Bitcoin y crear un número indefinido de bitcoins. Esta vulnerabilidad fue descubierta el 15 de agosto cuando se emitieron 184 000 millones de bitcoins en una sola transacción, pero fue detectada en cuestión de horas y borrada, siendo la vulnerabilidad arreglada. No ha vuelto a detectarse ninguna otra en el protocolo Bitcoin ni de ninguna de las otras criptomonedas importantes. Es decir, que la red de Bitcoin, excepto por este problema de seguridad, no ha sufrido nunca un ataque de ciberseguridad.

Los problemas como el de MtGox u otros, que frecuentemente aparecen en la prensa, son debidos a aplicaciones creadas por encima, como las *exchanges* o los monederos, que no se han desarrollado de forma segura y, por lo tanto, han dado lugar al acceso indebido de las claves privadas, las cuales a su vez dieron acceso a transferir bitcoins a otras direcciones distintas. Lo mismo podemos decir de la red de Ethereum: aunque ha habido multitud de problemas de seguridad en monederos como Parity o en operaciones de ICO, la red en sí misma nunca ha sufrido ninguna vulnerabilidad. Estoy convencido de que estos contratiempos se irán solucionando de manera progresiva conforme la industria madure y se vaya profesionalizando. Al fin y al cabo, ya ha pasado con el mundo bancario tradicional.

Hoy se escuchan pocas noticias de robos a bancos, pero no hace tanto tiempo, cuando yo era joven, todavía se producían asaltos a sucursales de forma frecuente, como el famoso intento de atraco al Banco Central en Barcelona en el año 1981. Así, al igual que ahora estos robos son algo residual en la sociedad actual, creo que pronto pasará lo mismo con los hackeos de las *exchanges* o los monederos de cripto.

La computación cuántica: la posible amenaza para las criptomonedas

Como hemos visto, la seguridad de las blockchains de las criptomonedas se basa en la inhabilidad de los ordenadores actuales de

resolver funciones criptográficas de forma eficiente. Tal es así que, si en el futuro los ordenadores pasan a ser varios órdenes de magnitud más rápidos, existe la posibilidad de que puedan resolver esos puzles criptográficos en poco tiempo y, por lo tanto, puedan llegar a manipular las criptomonedas.

Aquí es donde entran los ordenadores cuánticos como posible amenaza para las criptomonedas. Este tipo de ordenador usa un paradigma de computación completamente diferente al de la computación clásica. En el mismo, en lugar de bits se usan los llamados cubits, que pueden dar lugar a nuevos algoritmos de computación muchísimo más rápidos.

En la computación clásica, para incrementar la velocidad de computación de un ordenador se tiene que reducir el tamaño de los microchips para hacerlos cada vez más pequeños y así conseguir más velocidad de proceso. Sin embargo, existe un límite, ya que no se pueden hacer microchips infinitamente pequeños y a partir de cierto tamaño pierden sus propiedades y dejan de funcionar. En un ordenador cuántico, algo sobre lo que se teoriza desde los años ochenta, pero que aún no es una realidad, en lugar de jugar con unos y ceros como en la computación tradicional, se usa un estado más que el cero y el uno, un estado en el que una partícula puede ser un cero y un uno a la vez.

Hoy los ordenadores cuánticos están muy lejos de ser una realidad y los pocos experimentos existentes solo han conseguido una capacidad de computación extremadamente limitada. Por eso, a pesar de lo que defienden algunos expertos contrarios a las criptomonedas, no parece que vayan a ser ninguna amenaza para la seguridad de blockchain y las criptomonedas en décadas, si es que llegan a desarrollarse algún día, lo cual no está nada claro.

¿Excesivo consumo energético?

El elevado consumo energético por parte de los potentes ordenadores que en todo el mundo se dedican a los procesos de minería es otra de las críticas más habituales entre los opositores al bitcoin y las criptomonedas. «El Bitcoin

consume más electricidad que países como Dinamarca o Nigeria», son declaraciones que se han podido leer —o muy similares— en titulares de medios de comunicación.

Hay que admitir que el gasto energético de estos procesos es uno de los puntos débiles del protocolo inventado por Nakamoto a tener más en cuenta. Y es cierto también que una red descentralizada consume mucha energía porque se trata de ordenadores muy potentes que están funcionando veinticuatro horas y, además, la revaloración de la moneda hace que el incentivo derivado de la prueba de trabajo —que es como se conoce al sistema de consenso que se usa para estas redes— haga que la mayoría de los mineros no se anden con demasiados remilgos con respecto al gasto en electricidad y que la red continúe creciendo.

Ahora bien, ¿hablamos de un dispendio energético inasumible a medio plazo? Tampoco podemos cuantificar con exactitud el gasto energético, pues depende de la procedencia y la eficiencia energética de los equipos de los distintos mineros, pero admitiendo que es muy elevado —el investigador en políticas públicas Christopher Malmo calcula que cada transacción con bitcoin supone al menos veintiséis kilovatios hora en minería, o lo que es lo mismo, el 89 % de lo que consume un hogar medio estadounidense en un día—, también es necesario situarlo en contexto.

En términos absolutos el consumo eléctrico de la blockchain de Bitcoin vendría a significar apenas el 0,1% de lo que se consume en el mundo, y aunque compararlo, por ejemplo, con lo que consumen Dinamarca o Nigeria y situarlo por encima resulte llamativo, no deja de ser un tanto tramposo, ya que se trata de países con muy poca población, el primero, o escaso nivel de desarrollo, el segundo.

Si lo comparamos con otros países, la red de Bitcoin consume al día lo mismo que 520 000 canadienses; o bien, toda la electricidad consumida por Bitcoin en un año solo duraría diecinueve horas en Estados Unidos. Si fuera un país, se situaría en el puesto 117 de consumo eléctrico. Solo Google, con sus docenas de *data centers* enormes repartidos por el mundo en 2015, consumía ya el doble de electricidad que Bitcoin.

De manera que, parece que en el ámbito global, el consumo ni es tan alto ni resulta insostenible. Y tampoco nos engañemos: el consumo de la banca tradicional es obviamente mucho mayor. No olvidemos que el mantenimiento de las estructuras bancarias tradicionales tampoco nos sale gratis y el coste que implica la criptoeconomía bien puede verse como un precio razonable a pagar por la disrupción que provoca, por ser capaz de desintermediar un sistema

financiero que consume mucha más energía para llevar a cabo operaciones que van a dejar de ser necesarias, y que, además, nos cobran miles de millones de euros por prestar servicios que pueden ser reemplazados por otros muchísimo más baratos.

En cualquier caso, no obviemos que aquí reside un punto débil que habrá que considerar en el futuro y sobre el que se puede actuar. Tenemos margen de mejora. De hecho, otras blockchains como Ethereum y otras de tercera generación están trabajando precisamente en este terreno y buscando métodos criptográficos de consenso más eficientes desde el punto de vista energético, como enseguida veremos.

¿Fuente de especulación?

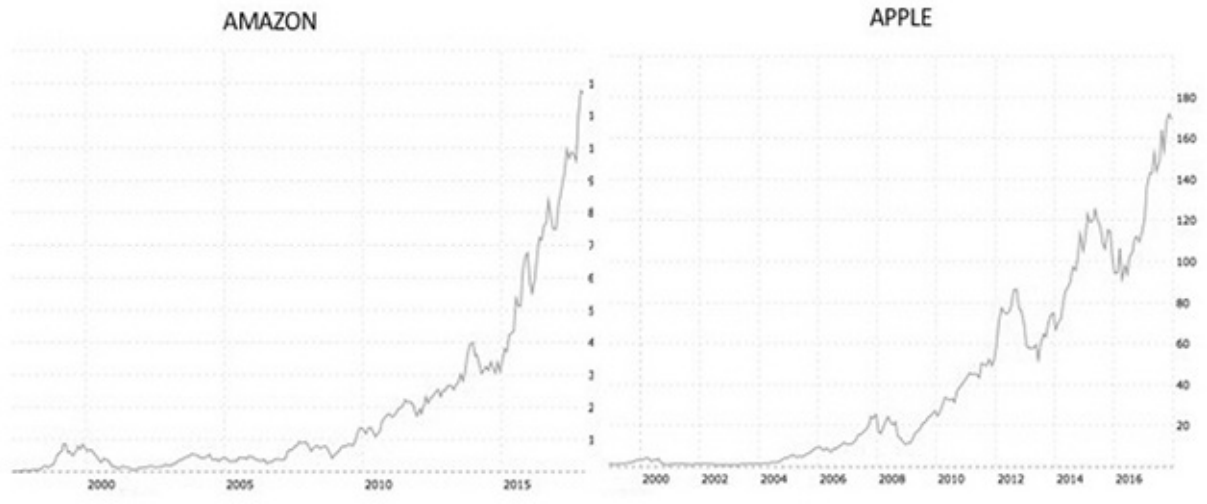
Otro de los lugares comunes en lo que a la criptoeconomía se refiere es el fuerte componente especulativo que se ha creado alrededor de ella. A mí me gustaría apuntar que el concepto especulador, aunque tiene una connotación negativa, no es más que el de un inversor dispuesto a asumir más riesgo que otro a cambio de un posible retorno mayor. Y que los especuladores, como inversores que arriesgan más que otros, son los que crean industrias nuevas, ya que invierten en las mismas cuando están en estado incipiente y poco desarrolladas y cuando su nivel de riesgo e incertidumbre es mayor.

Es normal que un mercado emergente y con tanto potencial como el de la criptoeconomía se llene de especuladores, pero eso no tiene por qué ser necesariamente malo, puesto que, como digo, son estos quienes en última instancia abren nuevos mercados y hacen fluir el dinero. Otra cosa es el abuso o que se ponga a especular cualquiera sin saber dónde se mete y sin criterios firmes de comportamiento, pero que ahora mismo haya en el mercado cripto muchos especuladores —llamémosles mejor inversores— que estén apostando y arriesgando su dinero por las criptomonedas, va a permitir el desarrollo de esta nueva realidad como antes ocurrió en otras industrias.

El ejemplo de Amazon es significativo. Durante la burbuja de Internet entre 1998 y 2000 el valor de la compañía estuvo por los suelos; se había desplomado su valor tras el pinchazo de la burbuja. Sin embargo, puesto que tenía detrás un buen sustento, una gran idea de negocio —fueron nada menos que los pioneros del *e-commerce*—, a lo largo de los años ha terminado generando un valor brutal que ya no es desde luego especulativo. No obstante, fue esa «especulación»

inicial la que le permitió ser lo que es hoy en día, ya que sin ella no hubiera sobrevivido.

Si miramos el gráfico de evolución en bolsa de Amazon, observaremos que esa famosa burbuja, cuando miras la evolución de la acción a más largo plazo, es prácticamente inapreciable. La especulación también crea industrias, y Amazon o Apple son ejemplos excelentes en este sentido.



Principios de 2000, cuando la burbuja del dot.com explotó.

Hemos de confiar que detrás de Bitcoin y blockchain también haya grandes ideas de negocio y un enorme potencial económico. No nos lamentemos antes de tiempo de una especulación que quizás está provocando un dinamismo en un mercado que necesitaba este movimiento. Para muchos puede que se esté generando una burbuja, pero otros vemos que esto, puesto en el lugar que le corresponde, lejos de ser una burbuja no es sino, como decíamos al principio, la punta de un gran iceberg.

LA PUNTA DEL ICEBERG

Muy en relación con esa dimensión especulativa que acompaña a la criptoeconomía emerge otra de las grandes críticas que se le hace: que estamos ante una burbuja que va a terminar por explotar más pronto que tarde.

Quería comentar esta cuestión al final del presente capítulo porque, en contraposición a esta idea que sobrevuela constantemente todo debate actual en

torno al bitcoin, las criptomonedas, los tokens o las ICO, deseo posicionarme en un punto completamente antagónico: lo que hemos vivido hasta el momento no es sino la punta de un iceberg que todavía está por descubrir sus auténticas dimensiones.

¿Estamos ante una burbuja?

Admitido que estamos en un periodo propicio a la especulación, es también posible que en el marco de esa euforia se estén produciendo operaciones asimilables a la creación de una burbuja, pero para entender realmente si esto es así, conviene poner las cosas en perspectiva y situar al bitcoin en su «lugar en el mundo financiero» para entender su tamaño actual y ver su potencial.

Así que nos va a resultar muy valioso medir cuánto de grande es el bitcoin con respecto a otros activos financieros, y evaluar si está justificada dicha posición o dicho tamaño en relación con su potencial.

De este modo, podemos darnos cuenta de que, aunque un bitcoin es ya muchas veces más valioso que una onza de oro, puesto que hay muchísimas más onzas de oro en circulación que bitcoins, el tamaño del mercado del oro es hoy en día muchísimo mayor. El oro representa aproximadamente un valor de más de 8 billones de dólares —un ocho seguido de doce ceros—, mientras que el tamaño del mercado del bitcoin estaba en marzo de 2017 por debajo de los 200 000 millones, es decir, unas cuarenta veces menos.

Dado que el oro crece con más rapidez que el bitcoin —ya que del primero se mina mucho anualmente del que se mina del segundo—, si en unos años este se convirtiera en un oro digital y reemplazara al oro actual como almacenamiento de valor y ese ocho con doce ceros se trasladara al bitcoin, el precio de este se dispararía de forma espectacular, superando su cotización con creces del medio millón de dólares desde los 10 000 dólares a los que está ahora. Es decir, tendría un crecimiento potencial de cincuenta veces.

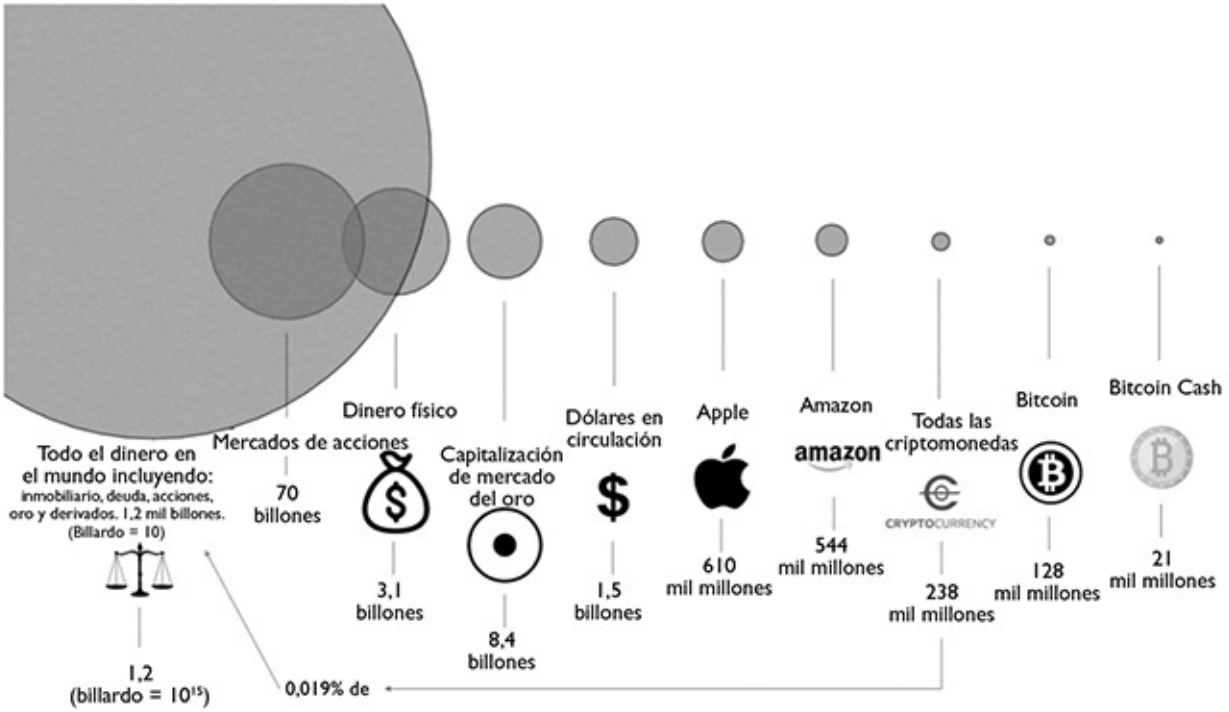
Además, el oro no deja de ser algo muy pequeño: solo las monedas de dinero fiat en el mundo acumulan un valor que supera en más de cinco veces el del oro. Podríamos añadir también otros activos financieros para seguir dándonos cuenta de las magnitudes de las que hablamos y de que el bitcoin no es aún sino una gota en el océano del mundo de las finanzas.

Por supuesto, puede ser que el bitcoin no triunfe y sea el Lycos de las criptomonedas, y que sea más tarde cuando aparezca el Google del cripto, pero a

lo que yo me refiero es que el valor de la criptomoneda que triunfe puede llegar a ser cincuenta veces mayor que el tamaño del bitcoin actual.

¿Tiene sentido hablar de burbuja dadas estas escalas? Si creemos que en un momento dado el dinero digital va a llegar a reemplazar al oro y potencialmente a las monedas, el valor del bitcoin hoy, lejos de representar una burbuja, es en realidad muy pequeño todavía.

El siguiente gráfico comparativo que ubica el bitcoin y el conjunto del mercado de criptomonedas en relación con otros activos financieros y al valor de algunas de las más importantes empresas actuales como Apple o Amazon, es ilustrativo.



Comparativa de criptomonedas, activos financieros y empresas.

Creo que queda patente que todavía hay mucho recorrido y mucho margen para el crecimiento de la criptoeconomía. Estamos hablando de una fracción mínima, y esto es extensible a las ICO, de las que todo el mundo habla, pero que, ya hemos dado antes estas cifras, apenas representan el 10 % de la financiación por *crowdfunding*, y ni siquiera el 1 % de lo que representa el capital riesgo anual.

También las ICO ofrecen un enorme margen para disrumpir. Y más cuando nos empecemos a mover de la emisión de tokens de utilidad para start-ups a tokenizar activos como los fondos o el mercado inmobiliario, que son mercados muchísimo más grandes y con muchísimo más potencial. Estamos empezando —todavía no es tarde para entrar en este mundo— y no tiene sentido escuchar a esas voces agoreras que solo ven una burbuja en lo que es una potencial revolución.

En definitiva, para terminar este capítulo y responder a las muchas críticas que se vierten sobre la criptoeconomía, es necesario recordar que todas esas nuevas oleadas de tecnologías disruptivas como Internet a finales de los noventa, los móviles a principios del siglo XXI, y ahora el mundo de cripto y blockchain, siempre vienen asociadas con una etapa de ebullición y especulación que, inevitablemente, viene luego acompañada de una caída. Pero también hay que tener en cuenta que, una vez pasada la misma, todas han seguido creciendo hasta hacernos olvidar las caídas, y todas han producido empresas que han transformado el mundo y el cómo hacemos las cosas, desde cómo accedemos al conocimiento, en el caso de Google, hasta cómo compramos, en el caso de Amazon, por poner dos ejemplos muy significativos.

Es posible que en el mundo cripto estemos ahora viviendo ese momento de burbuja o euforia especulativa, pero tengo claro que, a largo plazo, estas tecnologías están aquí para quedarse, y que van a transformar el mundo de cómo transaccionamos con valor tal y como la Internet actual ha revolucionado cómo transaccionamos con información o contenido.

En realidad, todavía está todo por hacer y hay cantidad de oportunidades. Las expectativas son altas y, por supuesto, hay unos cuantos retos a los que hacer frente que están marcando la evolución de este sector. Vamos a conocerlos.

8
AFRONTANDO RETOS: EL UNIVERSO CRIPTO 3.0

LOS GRANDES DESAFÍOS

Acabamos de ver que existen ciertos mitos y críticas en relación con la criptoeconomía que resultaban conveniente matizar, pero eso no significa que, en efecto, no haya aspectos que son mejorables y que constituyen retos necesarios de afrontar. Tal es así que el futuro de la criptoeconomía tiene mucho que ver con cómo son desafiados estos, que en buena medida llevan cierto tiempo sobre la mesa. En la respuesta a los mismos es donde identificamos las nuevas propuestas de criptomonedas y blockchains de la que sería ya la tercera generación cripto, y que enseguida vamos a conocer.

Los principales retos a los que se enfrenta la criptoeconomía ya han sido presentados en estas páginas, y se refieren a su escalabilidad y su volatilidad, aunque cabe añadir otros como la interoperabilidad o la usabilidad. En las respuestas que se están dando a estas cuestiones, especialmente a las dos primeras, se percibe la evolución y el potencial de esta tecnología tan innovadora y disruptiva de la que venimos hablando.

Tal es así que podemos afirmar que las blockchains de tercera generación están desarrollando soluciones para mejorar la escalabilidad con respecto a Ethereum, a la que nos referimos como blockchain 2.0, mientras que muchas de las nuevas criptomonedas que ven la luz nacen con vocación de superar esa volatilidad que arrastra el bitcoin desde su irrupción.

Detengámonos un poco en estos grandes retos que se le presentan a la criptoeconomía, porque esa es la mejor manera de ser capaces de anticipar su futuro.

ESCALABILIDAD

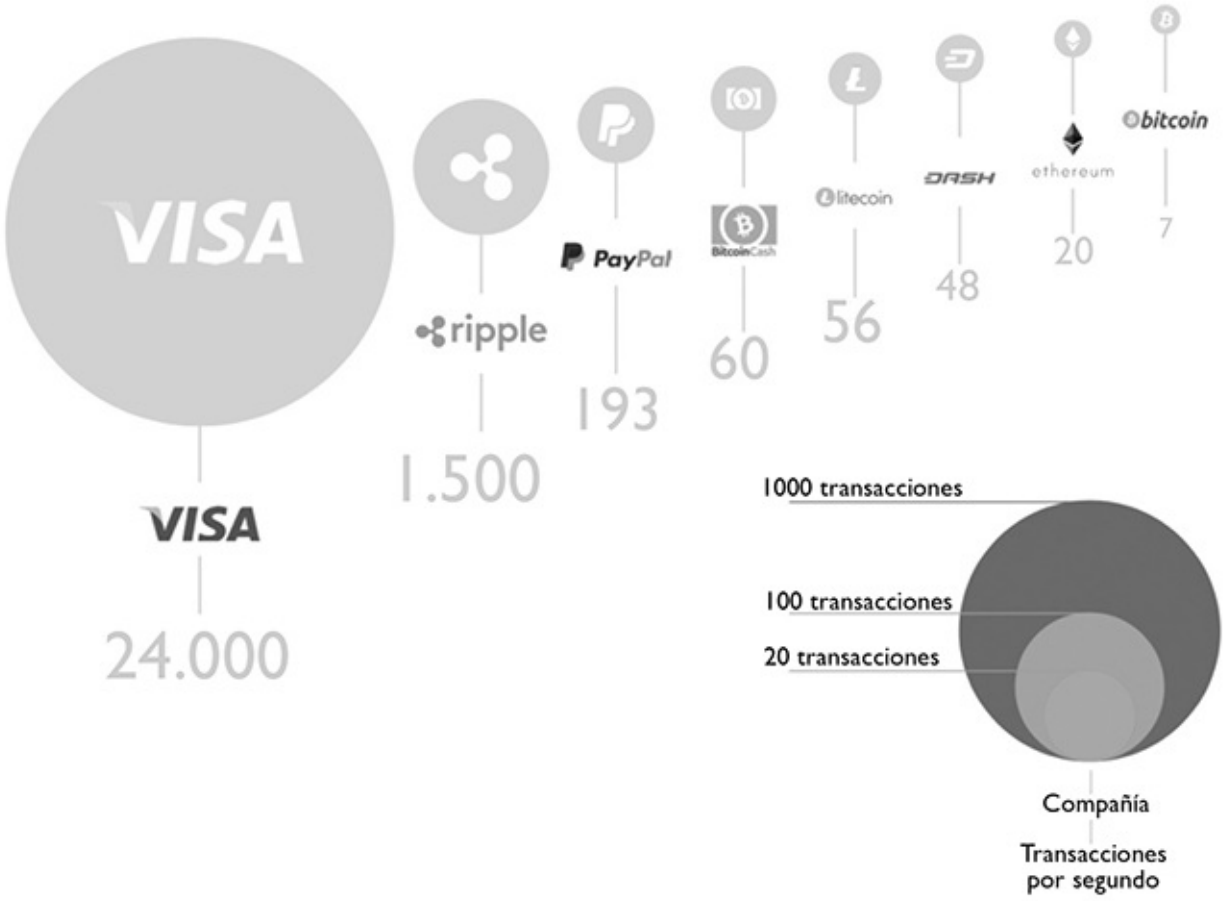
Seguramente este es el reto más importante al que hacen frente las criptomonedas y, de hecho, una de las grandes preguntas que se formulan en este mundillo es si las hoy blockchain líderes, Bitcoin y Ethereum, «lo conseguirán», es decir, si saldrán airosas de este desafío de la escalabilidad.

Ya hemos hablado antes de la cuestión. La realidad es que, al haber crecido tanto, al añadir tantas transacciones con bloques cada pocos minutos, a menudo las transacciones tardan en ser verificadas y registradas. Por diseño, la tecnología de blockchain tiene más problemas de escalabilidad que un software centralizado porque, como sabemos, todos los ordenadores han de contribuir a verificar y registrar las transacciones. Al contrario de lo que ocurre con los ordenadores centralizados, en una blockchain cuantos más ordenadores haya, más se ralentizan los procesos. Es el precio que hay que pagar por la descentralización y la inmutabilidad.

En general, cuando se diseña una blockchain hay que tener algún tipo de balance para conseguir de manera simultánea tres cosas: descentralización, consenso y escalabilidad. Como estamos viendo, las blockchains son capaces de lograr consenso sobre el estado de un activo o moneda de forma completamente descentralizada, pero esto ha sido a costa de perder escalabilidad. Hoy Bitcoin procesa tan solo siete transacciones por segundo, por las veinte de Ethereum, mientras que el —relativamente— recién creado Bitcoin Cash hace sesenta, acercándose a PayPal, capaz de hacer ciento noventa y tres transacciones por segundo.

Sin embargo, en todo caso esto palidece en comparación con la capacidad del mundo financiero tradicional. La red de procesado de pagos con tarjetas de Visa puede llegar hasta 24 000 transacciones por segundo. En el mundo de blockchain, el líder en escalabilidad es por ahora mismo Ripple, con 1500, pero ya hemos visto que lo hace a costa de sacrificar la descentralización, y, por lo tanto, no se puede comparar con los esfuerzos de escalado de redes como Ethereum o Bitcoin, que lo pretenden hacer manteniendo esta descentralización.

Por añadidura, ya sabemos que la mayoría de las blockchains se basan en el método de consenso llamado *proof-of-work* (PoW), o prueba de trabajo, que exige ordenadores muy potentes y muy caros, y consumen asimismo gran cantidad de electricidad, conectando así con uno de los problemas atribuibles a la criptoeconomía que citábamos anteriormente.



Velocidad de transacción de las criptomonedas comparadas con Visa o PayPal.

De manera que nos encontramos con problemas estructurales de diseño —que tienen que ver con el tamaño del bloque y el tiempo de emisión— y con dinámicas complejas, como que cada transacción deba ser verificada por la red entera y sometida a una prueba de trabajo para llegar al consenso de cómo aceptarla y validarla de forma distribuida, lo cual implica un muy alto consumo energético.

Así las cosas, hemos de admitir que, tal y como están diseñadas las blockchains de Bitcoin o la de Ethereum, la verdad es que no van a conseguir escalar nunca, y por eso tienen que evolucionar.

¿Cómo es posible superar estos problemas de escalabilidad? Principalmente se proponen tres soluciones. La primera pasaría por intentar crear sistemas donde se puedan realizar las transacciones de forma muy rápida en una capa paralela a esa blockchain principal donde, como sabemos, se almacenan todas las

transacciones. De esta forma, estas se consumirían por fuera y periódicamente se introducirían en la cadena principal.

Por otro lado, se propone sustituir la *proof-of-work* (PoW), o prueba de trabajo, por la llamada *proof-of-stake* (PoS), o prueba de participación. En ambos casos hablamos de protocolos de consenso distribuido, pero la segunda incorpora alguna novedad que hace que la obtención de la recompensa no dependa tanto del poder computacional del minero y no exija en consecuencia tanto consumo.

Como hemos visto en los primeros capítulos, los algoritmos de consenso son una parte fundamental de lo que hace que una blockchain funcione, ya que dictaminan cómo se verifican y ordenan las transacciones en un libro mayor distribuido. Sin una entidad central, la red de participantes —nodos, mineros— que conforman una blockchain tienen que ponerse de acuerdo acerca de la validez de las transacciones que se añaden al libro mayor, usando una serie de reglas predeterminadas.

La idea es que, se use el método que se use para resolver este problema —el conocido desde los años ochenta como el problema de los generales bizantinos —, se tiene que hacer de forma que ningún actor individual o —grupo de actores — que se una para intentar modificar el libro mayor tenga suficiente poder como para manipularlo.

El primer método de consenso distribuido que surgió en la era cripto con el bitcoin fue el llamado *proof-of-work* o prueba de trabajo. Como hemos visto, consiste en que cada nodo intente resolver un problema criptográfico usando sus recursos computacionales, siendo el que lo resuelve quien tiene el derecho a validar la transacción —o el bloque de transacciones, más precisamente— y escribirla en la cadena de bloques que, a su vez, el resto replica. Esto es lo que provee de la propiedad de inmutabilidad al libro mayor, ya que una vez escrita por todos, solo se puede modificar si la mayoría lo acepta, algo bastante complicado de que pase en un sistema con muchos nodos y una alta descentralización.

Pero como sabemos, el problema de esta solución es el alto consumo de recursos computacionales que se traduce en un alto consumo de energía, algo que no termina siendo muy sostenible. La alternativa propuesta por la industria es la prueba de participación que surge en el año 2012. Esta se sustenta en la suposición de que, en lugar de basarnos en comprar un hardware caro para poder resolver pruebas criptográficas más rápidas que el resto y tener el retorno económico de las mismas, quienes posean más unidades de una moneda basada en PoS serán quienes estén especialmente interesados en su supervivencia y

buen funcionamiento, de manera que serán ellos los más indicados para cargar con la responsabilidad de proteger al sistema de posibles ataques. Por eso, el protocolo los premia con una menor dificultad para encontrar bloques, dificultad que sería inversamente proporcional al número de monedas que demuestren poseer. Dicho de otro modo: cuantas más monedas tienes ya, más puedes participar y más posibilidades dispones de obtener retorno. Otro factor que se tiene en cuenta es cuánto tiempo hace que poseen las criptomonedas, para premiar también a los nodos que están invertidos en el funcionamiento a largo plazo de la red.

Lo cierto es que no es un funcionamiento sencillo y hay bastantes problemas por resolver —en particular el llamado *nothing at stake*, donde si hay una bifurcación, un nodo puede estar minando en dos blockchains a la vez, ya que tiene monedas de ambas, y no apuesta por ninguna—, pero con todo, estamos ante algo que se está comenzando a implementar cada vez más, y una línea en la que están trabajando las blockchains 3.0 que se diseñan ya directamente así.

Incluso la propia Ethereum ha anunciado que va a migrar de PoW a PoS, aunque no está claro exactamente cuándo. Otras variaciones que se han contemplado son las llamadas *delegated proof-of-stake* (DPoS en sus siglas en inglés) o prueba de participación delegada, que ha sido promovida por Dan Larimer, el co-fundador de BitShares, Steemit y EOS. Esta prueba usa unos grupos de delegados que son seleccionados por la red de usuarios y que tienen unos nodos separados para hacer el minado. Como estos delegados se consideran fiables por la comunidad, esto soluciona el problema del *nothing at stake* descrito anteriormente.

Todo esto nos demuestra que la búsqueda de un mecanismo de consenso ideal que tenga en cuenta el coste, la eficiencia y la escalabilidad continúa siendo unos de los problemas sin solucionar de la comunidad blockchain, por lo que la industria todavía tiene ante sí el enorme reto de conseguir consenso descentralizado de forma eficiente y rápida.

Pero hay una tercera vía para solucionar los problemas de escalabilidad que consistiría en realizar las transacciones *off-chain* —fuera de la cadena— en lugar de *on-chain* —dentro de la cadena—.

Hoy, para registrar una transacción todos los nodos deben hacerlo, pero la propuesta de futuro sería que existieran cadenas más ligeras que registraran solo una parte de las transacciones entre dos entidades, abriendo una especie de canal de pagos entre ellos, y no todo el histórico cada vez, aunque luego, obviamente, cuando se cierre ese canal, los registros deban ser trasladados a la cadena

principal para que hubiera consistencia. Si esto se pudiera hacer de forma segura, evitando el problema del doble gasto, se ganaría muchísima escalabilidad. En realidad, es un modelo que se asemeja a lo que viene haciendo Visa. Desde que uno paga con su tarjeta hasta que ese dinero es transferido a la cuenta del receptor pasa cierto tiempo. El concepto sería el mismo: que se pudiera garantizar que la transacción ha pasado y no se pudiese deshacer, admitiendo que hasta que esté copiada en el libro mayor distribuido pueda haber un pequeño espacio temporal que no genere un problema de doble gasto.

Asegurar que esto pase se consigue con una serie de *smart contracts* que garantizan que ese dinero se mueva solo entre esas dos entidades. Es lo que se conoce como *Lightning Network* —red de la luz—, que está ya implementado en algunas blockchains como la de Litecoin, y se ha empezado a experimentar con ella en Bitcoin y Ethereum. El nombre viene de la rapidez a la que pueden pasar las transacciones: la velocidad de la luz. Con este sistema se pueden mover las transacciones fuera de la blockchain pública y hacerlo solo entre dos entidades, consiguiendo, además de incrementar la velocidad en la transacción, abaratar mucho los costes de la misma, ya que los mineros no están involucrados y, por lo tanto, no cobrarán nada por hacerlas. Estas redes paralelas a la blockchain pública principal están diseñadas para conseguir soportar micropagos con criptomonedas como bitcoin, algo que hoy por hoy no es factible por el tiempo que tardan y el coste que tienen.

INTEROPERABILIDAD

Hoy en día no hay una manera sencilla de que de un bitcoin pases a un ether, o de que un *smart contract* ejecutado con la blockchain de Ethereum sea válido para otra… Uno de los inconvenientes que Internet solucionó en su momento fue el de la interoperabilidad, por ejemplo, entre direcciones de correo electrónico —no existe ninguna dificultad en enviar un *mail* desde una dirección de Gmail a, por ejemplo, una de Hotmail—. Sin embargo, en el mundo blockchain no hay prácticamente interoperabilidad, y eso termina generando un problema, porque al final el universo cripto está construido a base de muchas islas —blockchains — diferentes, y no resulta fácil moverse de una a otra.

La idea sería conseguir una especie de «Internet de blockchains» donde todas hablen con todas de alguna forma. De las nuevas iniciativas que venimos enumerando, esta es la que con diferencia está más verde de todas. Uno de los

principales actores en estas iniciativas, una compañía llamada Polkadot, no tiene pensado empezar a operar hasta 2019. Los métodos empleados para introducir interoperabilidad entre blockchains varían, pero normalmente se focalizan en aspectos como el poder realizar transacciones de una blockchain a otra de forma segura, crear blockchains que aseguren la interoperabilidad entre otras dos de ellas o puentes que ofrezcan conexiones de una blockchain a otra.

USABILIDAD

Reconozcámoslo: ahora todos hablamos de dinero digital y de bitcoins, pero al margen del entorno de esos libertarios y ciberpunks y de los entusiastas de la tecnología que suelen ser usuarios tempranos de todas las cosas —como me pasa a mí—, su uso no está todavía nada expandido. Y una de las principales barreras de entrada es que de momento la usabilidad de muchos de los servicios disponibles es bastante baja. Esto nos puede recordar a los inicios de Internet, con una usabilidad muy baja de casi todos los servicios, y cuando el mero hecho de conectarse usando un módem y un software especial para hacer la llamada era todo un reto. Hoy, comprar o vender bitcoins u otra moneda, crear monederos de Ethereum para guardar tokens o participar en una ICO no está en absoluto diseñado para todos los públicos.

Ahora mismo esto de las criptomonedas y su compraventa se reduce a un proceso especulativo a la espera de lo que ocurra en el futuro, más que a una auténtica utilidad práctica que se le pueda dar a las monedas. Hay algunos usos muy concretos en transferencias, incluso algunos pagos, pero en realidad muy pocos todavía.

Como ya apuntamos en el segundo capítulo, una de las compañías que más éxito está teniendo precisamente por su sencillez y buena usabilidad es la *exchange* americana Coinbase, pero quizás sea Ethereum la que tenga más aplicación práctica por lo que rodea a los tokens de las ICO, que usan la moneda de Ethereum y hacen que sea la única que tiene cierta correlación entre su aplicación y el valor de su moneda, así como con la cantidad de proyectos desarrollados en su red de blockchain para la creación de aplicaciones descentralizadas.

Otro aspecto importante de la usabilidad es cómo de usable sea no ya para los usuarios, sino para los desarrolladores. Es decir, estaríamos hablando de cómo de sencillo es de desarrollar, cómo de completa es la documentación, qué

herramientas de desarrollo existen, etc. Que sea más fácil para ellos desarrollar aplicaciones —*Dapps*, en este caso— hará que la blockchain tenga más valor.

De manera que en el momento presente, dentro del universo blockchain, estamos a esos niveles mínimos de usabilidad, muy lejos de los de Facebook, Uber y otras muchas aplicaciones que todos conocemos o de las herramientas de desarrollo de compañías como Microsoft. Es un terreno que, a pesar de la irrupción del componente más especulativo, está todavía un poco abandonado. Estamos en un momento aún muy emergente y las criptomonedas no han llegado a ofrecer servicios «usables» para los ciudadanos. Claro que influye también mucho la volatilidad del dinero digital. Y con esto llegamos a otro de los grandes retos a los que se enfrenta la criptoeconomía.

VOLATILIDAD

Lo hemos comentado ya varias veces: el bitcoin o las criptomonedas en general no pueden ser consideradas en la actualidad auténticas monedas en el sentido de que no cumplen las tres condiciones que les exigimos: sirven como almacén de valor, pero no como medio de intercambio ni como referencia de precio. Y esto es debido sobre todo a su volatilidad. No hay más que repasar la evolución de su cotización; y no necesariamente a lo largo de sus años de existencia, con mirar el último es suficiente. Como sabemos bien, la oferta limitada de una moneda deflacionaria como esta provoca que, ante los fuertes incrementos y descensos de demanda que se vienen produciendo, se generen cambios bruscos en su cotización: la moneda es volátil.

De manera que, precisamente una de las cualidades más apreciadas en el bitcoin u otras criptomonedas, esa escasez que nadie puede manipular produciendo más como ocurre con el dinero fiduciario, se convierte en este caso en su peor enemigo.

Mientras este problema no se solucione, será muy complicado que el bitcoin, la criptomoneda pionera, pueda ir más allá de su dimensión de oro digital y se convierta en una moneda completa y válida para ser usada de forma normalizada para realizar pagos. Y es por eso que de cara al futuro viene ganando mucha fuerza la creación de otras monedas que se diseñan con el objeto de superar este reto. Son las *stablecoins* o criptomonedas estables.

SE BUSCA CRIPTOMONEDA ESTABLE PARA REALIZAR PAGOS

Nos hallamos ante el enorme reto de encontrar una moneda digital cuya volatilidad pudiera ser minimizada a partir de una organización autónoma descentralizada —es decir, la idea es seguir prescindiendo de una autoridad central—. Y es con esa premisa que emergen esta categoría de activos digitales llamadas *stablecoins*.

Aquí, de lo que estaríamos hablando es de criptomonedas que buscan continuar con la idea de la descentralización, es decir, que no sean emitidas por una autoridad central, pero a la vez, que sean capaces de producirse bajo criterios de oferta más flexibles, lo cual les permitiría no ser tan volátiles.

Se trataría de algo similar a lo que hacen los gobiernos cuando emiten deuda pública y la venden, provocando que se incremente el flujo de dinero en el mercado y manteniendo los precios estables. Por otro lado, la habilidad de los gobiernos de alterar la política monetaria y la cantidad de dinero existente emitiendo más es, precisamente, uno de los aspectos criticados en la economía actual, ya que devalúa al consumidor y al ahorrador.

Por supuesto, ello no es posible con la política monetaria del bitcoin, pues es determinista y está fijada de antemano, pero si se consiguiera desarrollar una moneda digital que no tuviera esta política y que pudiera emitirse según la oferta y la demanda existente para que su valor no fuera tan volátil, estaríamos dando un paso de gigante para que tal moneda fuera un medio de pago válido y normalizado.

En la actualidad se trabaja mucho en este campo, y las soluciones o modelos que se están planteando son diversos. En primer lugar, se propone que la moneda se emita de forma centralizada y respaldada por un activo que se guarde conforme se emiten monedas nuevas. Esto se conoce en el mundo financiero como emitir una IOU —o *I owe you*, ‘yo te debo’—, que quiere decir que hay un activo por debajo de otro que «se debe», y eso garantiza su valor subyacente. El ejemplo más conocido de este tipo de *stablecoin* es tether, una criptomoneda que establece su paridad con el dólar.

Establecer esta equivalencia entre la moneda digital y el dólar significa que se guardan tantos dólares como monedas se emiten, y si se quieren emitir más, habrá que reservar más dólares. De este modo, sirve para hacer compras digitales fuera del sistema bancario tradicional, pero con una estabilidad en la referencia de valor. Tether, además, ayuda así a que muchas *exchanges* permitan la compraventa de bitcoins usando tethers como algo intermedio entre el dólar y el

bitcoin, sin tener una licencia por recibir y custodiar dinero de terceros. Sin embargo, esta criptomoneda no está exenta de polémica, ya que no está muy claro que en realidad se tengan los dólares por los tethers que están emitiendo. Existen serias dudas en el mercado, y es que al estar basado en un activo centralizado no solo rompe con la filosofía cripto de partida, sino que, además, se intensifica el riesgo de que pudieran estar manipuladas por la falta de descentralización en el protocolo.

Otra de las opciones es el llamado respaldo colateral descentralizado. Se trataría de emitir criptomonedas amparadas por activos descentralizados —por ejemplo, emitir una moneda con la protección del propio Bitcoin o Ethereum—. La ventaja de esto frente a hacerlo con el dólar es que se puede intentar automatizar y realizar de forma descentralizada el proceso de emisión de monedas estables, así como de mantenimiento del colateral contra la moneda estable, los niveles de colateral que se pide, etc., ya que está hecho dentro del mundo cripto y digital.

Sin embargo, tiene otras desventajas que lo hacen complicado de gestionar, puesto que el propio activo que pones por debajo es volátil, no es estable en sí mismo, así que es previsible que esto impacte a la estabilidad de la moneda que emites o en la cantidad de colateral que es necesario mantener, el cual suele ser bastante alto para protegerse de la eventualidad de un cambio brusco de precio. Normalmente, para que estos esquemas funcionen hay que asumir que los precios de la cripto que se usa como colateral siempre están subiendo, o si no tendrás un exceso de colateral que los hace poco prácticos. El ejemplo más conocido es una moneda que se llama dai, emitida por la empresa Maker DAO.

Y, por último, se trata de la posibilidad más interesante, aunque a la vez la más complicada de implementar. Se plantea un modelo basado en un algoritmo que automáticamente y de forma descentralizada regula el suministro de la moneda según la oferta o demanda que haya de la misma en el mercado, para que de este modo se mantenga estable en cuanto al precio. Sería lo más parecido a lo que hace un banco central, pero de forma descentralizada, algorítmica y automática. El ejemplo más conocido de estas monedas es Basecoin.

Lo cierto es que, hoy por hoy, no está claro que ninguna de estas ideas esté funcionando, y todavía nos encontramos en una fase de búsqueda de esa criptomoneda que nos permita realizar pagos, pero, sin duda, este reto está marcando el futuro de las criptomonedas del mismo modo que el reto de la escalabilidad está marcando el diseño de las blockchains de tercera generación. Lo que está claro es que hay una necesidad de monedas más estables y que la

creación de las mismas es una tendencia que va cada vez a más, y un espacio al que hay que estar muy atento en el futuro.

BLOCKCHAINS DE TERCERA GENERACIÓN

Hablábamos en la segunda parte de este libro de lo que significó la aparición de Ethereum y todo el abanico de posibilidades que abrió al introducir la posibilidad de programar también aplicaciones completamente descentralizadas y permitir que a las transacciones que se registran en los nodos de la tecnología blockchain se les pudieran añadir o programar otras propiedades. Irrumpieron de este modo los *smart contracts*, los tokens y las ICO, permitiendo que la revolución financiera fuera mucho más allá de lo que existía con las primeras blockchains como Bitcoin o sus derivados, que están dedicadas a ser estrictamente criptomonedas y no plataformas de aplicaciones distribuidas.

Por eso decimos que con Ethereum nacía la blockchain 2.0, o la segunda generación de plataformas cripto. Sin embargo, estamos en un punto que vamos un paso más allá, y empieza a asomar su cabeza una nueva generación de blockchains, plataformas de aplicaciones distribuidas que buscan superar los problemas de escalabilidad y otros que todavía padece Ethereum, algunos de los cuales ya hemos mencionado en la parte anterior.

Así pues, sobre esta escalabilidad se centra el principal campo de trabajo de las nuevas generaciones de blockchain. Se siente en buena medida que va a ser esta tercera generación la que en realidad llegue para quedarse, aunque de momento todavía hay mucha diferencia de tamaño y madurez entre Bitcoin, Ethereum, Ripple o Litecoin y las de tercera generación que están empezando. No obstante, en la comunidad se siente que hay expectativas de que una de estas en breve vaya a disrumpir y se convierta en el próximo Ethereum. De ahí que muchas tengan criptomonedas con un alto valor, por encima de los miles de millones de dólares, y situadas entre las más valiosas. Así que repasemos las más significativas o que más atención están focalizando.

Una de las plataformas que está dando más que hablar como la 3.0 para ser la próxima Ethereum es Cardano (ADA). De hecho, es la única de tercera generación que se coloca entre las cinco más importantes y supera ya en capitalización de mercado a Litecoin.

Cardano está fundada por Charles Hoskinson, una persona muy reconocida en la industria, ya que fue co-fundador de BitShares y de Ethereum. La principal

novedad de Cardano es haber introducido un algoritmo de participación (PoS), en vez de la tradicional prueba de trabajo (PoW), conocido como Ouroboros, el cual facilita la creación de cadenas laterales y permite la delegación en función de la participación del usuario. Ofrece, además, un lenguaje de programación de más calidad para los *smart contracts*, que bien podría sustituir al de Ethereum, dando paso a los contratos inteligentes de siguiente nivel y evitando muchos de los *hacks* que han sufrido las aplicaciones desarrolladas en Ethereum.

Otra de las pioneras en la introducción de la PoS fue EOS, fundada, como ya hemos dicho, por Dan Larimer, que fue co-fundador de dos blockchains bastante exitosas como BitShares —una plataforma financiera descentralizada cuyo otro fundador es el de Cardano— y Steemit —una plataforma de red social descentralizada con un sistema de pago para quienes postean cosas populares y reciben *likes*— e inventor, como hemos visto antes también, de la versión delegada de PoS.

Desde EOS han hecho una ICO muy exitosa que les ha permitido recaudar dinero durante todo un año —de hecho, en el momento de la publicación del presente libro todavía no se ha culminado dicha ICO—, lo suficiente como para tener la capacidad de crear un ecosistema propio notablemente exitoso. Otro de sus potenciales hace, además, referencia a su usabilidad, no solo referida a usuarios, también para desarrolladores —por ejemplo, Ethereum no resulta nada amigable para desarrolladores, y EOS pone el foco en esto—.

Otras criptomonedas 3.0 que son interesantes citar son NEO, NEM, Stellar o IOTA. La primera está focalizada en la digitalización de activos y la escalabilidad, y se está convirtiendo en la plataforma de blockchain de referencia en China, su país de origen.

NEM, por su parte, merece ser apuntada entre las blockchains de nueva generación porque usa un modelo de consenso llamado *proof-of-importance* (PoI), o prueba de importancia, donde el peso en la red no depende solo de la cantidad de monedas que se tengan —como en PoS—, sino también de cuántas transacciones se realicen. No hace mucho NEM ha estado en la mirada de todos, ya que ha sido la plataforma escogida por el gobierno de Venezuela para crear su criptomoneda respaldada por barriles de petróleo llamada petro.

Stellar, fundada por el creador de Ripple cuando dejó esta, busca trasladar las posibilidades tecnológicas de Ripple, que prescinde de los procesos de minería, aunque a diferencia de ella, lo hace con proyección de plataforma de blockchain pública, y no privada y centralizada. Dada la popularidad y el prestigio de su

fundador, es una plataforma de blockchain que tiene bastantes seguidores y que, además, ya está funcionando.

Finalmente, también debemos citar IOTA, focalizada en el hoy en día tan en boga Internet de las cosas, y que es la décima criptomoneda del mundo. Con esta de tercera generación lo que se da es un paso tecnológico más allá, al buscar alternativas para el universo cripto diferentes a blockchain. Es decir, en un sentido estricto, IOTA no es una blockchain y no tiene mineros ni coste de transacción, y cualquier nodo puede realizar una transacción tan solo verificando otras dos. Su idea innovadora es que aplicaciones de la Internet de las cosas donde los miembros de la red son elementos con poca capacidad de computación —por ejemplo, la nevera de casa— tengan su propia identidad y su propio monedero y, por ejemplo, puedan encargar y pagar leche cuando se les acabe para que la envíen de forma automática. Esto, como te puedes imaginar, abre un mundo de posibilidades enormes de aplicaciones nuevas que se pueden desarrollar.

No sabemos aún si Bitcoin o Ethereum habrán de ser suficientemente ágiles a la hora de incorporar modificaciones y mejoras, o serán nuevas criptomonedas de tercera generación las que ganen la partida, las Google y Facebook del universo cripto frente a unas Bitcoin y Ethereum que pueden quedarse con la función que cumplieron en su momento Netscape o Lycos.

Y es que son muchos los que piensan que las pioneras arrastran ya demasiado lastre histórico y no van a ser ya capaces de escalar, mientras que las nuevas blockchains nacen sin mochila y se diseñan desde cero con el cometido de afrontar los retos que no han sabido solventar todavía Bitcoin o Ethereum. O quizás sí cabe confiar en las que lo han revolucionado todo, y Bitcoin y Ethereum no sean Netscape o Lycos, sino las Amazon y Microsoft de la criptoeconomía, empresas que sí han sobrevivido a los diferentes cambios tecnológicos y avances, y que se han ido reposicionando con el paso del tiempo.

No es fácil pronunciarse ahora mismo en este sentido. Pero no cabe duda de que con las pioneras abriendo camino y con las nuevas generaciones aportando mejoras se ha abierto una brecha de disrupción tecnológica que tiene todos los visos de convertirse en una auténtica revolución financiera y económica.

9
DE LA DISRUPCIÓN TECNOLÓGICA A LA REVOLUCIÓN FINANCIERA

UNA CASA EN EL EXTRANJERO

Yo quiero imaginar un futuro en el que la compra de mi casa en Castellón hubiera podido ser de una manera bien distinta. Estoy volviendo al principio de este libro, a aquella experiencia personal que me resultó tan ilustradora de cómo la realidad puede transformarse radicalmente para bien gracias a la innovación tecnológica que nos trae blockchain y el universo cripto.

Como ya sabes, la compra de la casa en España cuando yo residía fuera representó para mí un proceso lleno de incomodidades, mucho tiempo perdido y demasiados gastos innecesarios. La operación implicaba enviar dinero desde el extranjero a España, y eso hoy por hoy dentro del sistema bancario tradicional implica una serie de gastos desorbitados y el empleo de un tiempo francamente excesivo. Además, para poder comprar la casa me vi obligado, entre otras cosas, a acudir presencialmente a un banco para que me emitieran dos cheques: uno por la cantidad que había que embolsar al vendedor y el otro para liberar la hipoteca que todavía pesaba sobre la propiedad. Sobra decir que, la verdad, la mera emisión de estos cheques me costaron un dineral, cuando no dejaban de ser un par de papeles con una firma impresa que demostraban que yo tenía el dinero y que podía acceder al mismo. Después, además de acudir al banco a por los cheques y pagarlos, fue necesaria una reunión presencial con el notario, a quien, por supuesto también hubo que pagar, en la que nos juntábamos compradores y vendedores y la persona del banco que aún tenía una hipoteca pendiente del anterior dueño. De nuevo un excesivo esfuerzo de coordinación e incomodidades. Como ya he proclamado antes desde estas páginas, que tengamos que pasar hoy por un proceso así es sencillamente arcaico e innecesario. Por eso propongo que nos imaginemos un futuro en el que todo sea

cripto y blockchain. El escenario que viviríamos para realizar la compra de esa casa sería bastante diferente.

Básicamente, toda la operación se hubiera realizado de manera automática mediante el empleo de *smart contracts* y unos monederos seguros que pudieran enviar el dinero en cripto de forma casi instantánea y con unos costes de transferencia bajísimos —y además, independiente del país, de modo que el proceso funcionaría exactamente igual estuviera donde estuviera el comprador —.

El *smart contract* actuaría de fideicomiso y guardaría el dinero de la compra. Con una parte liberaría la hipoteca y con la otra pagaría el resto al vendedor. También registraría el cambio de la propiedad de la casa hacia mí de forma mecánica, y aseguraría la transferencia de dinero encriptado de manera completamente segura en cuestión de segundos. Ni los cheques, ni la intervención del banco ni la del notario hubieran resultado necesarios. Todo seguro, rápido y descentralizado. Y, además, el título de propiedad quedaría registrado en la blockchain de forma inmutable para que se supiera que la casa es mía hasta que decidiera venderla.

Por supuesto, necesitaríamos que los agentes inmobiliarios del futuro fueran los que realizaran los desarrollos necesarios por encima de una blockchain para que el proceso anterior fuera posible, y también alguien tendría que auditar los *smart contracts* para asegurarse que hacen lo que dicen —los abogados del futuro—, pero ya hay mucha gente trabajando en eso, y efectivamente ya se han comprado varias propiedades en el mundo usando cripto.

Que esto se hubiera hecho de manera segura, automática, descentralizada, fiable y sin apenas gastos es completamente revolucionario que el futuro nos ha de traer. Hablamos de la transacción de valor y de confianza. El impacto transformador y las implicaciones de esto tienen un alcance inimaginable que va a disrumpir no solo el sector financiero; sus ramificaciones van a alcanzar en buena medida toda nuestra realidad empresarial y económica. Por eso digo que desde la disrupción tecnológica que trae consigo la tecnología blockchain llegamos a una revolución financiera, empresarial y económica.

Por supuesto, como suele pasar muchas veces con la aparición de nuevas tecnologías, también tiene connotaciones negativas, principalmente la pérdida de empleos. Por un lado, el impacto para el sector financiero y bancario podría ser tremendo, muy superior al que ya tuvieron con la aparición de los cajeros automáticos primero, y, más adelante, con la digitalización de sus operaciones, de forma que se pudiera operar con ellos sin ir a una sucursal —de hecho, yo

creo que la primera vez que iba en años fue para que me hicieran los cheques de la compra de la casa que mencionaba arriba—. Pero también impactaría en otras profesiones: notarios, abogados o incluso los agentes inmobiliarios o agentes del registro. Algunos empleos se tendrán que transformar; su rol seguirá siendo necesario, aunque diferente —¿quién escribe y audita el *smart contract* de la compra de una vivienda?—, pero otros desaparecerán por completo.

Por supuesto, no es la primera vez que en la historia de la humanidad muchas profesiones desaparecen debido a las mejoras tecnológicas —el lechero que repartía la leche, las operadoras de telefonía que nos conectaban la llamada o el farolero que encendía y apagaba la iluminación pública de las ciudades, por poner unos ejemplos—, pero estas no impactaron normalmente en la tasa de desempleo a largo plazo. Sin embargo, hoy la tecnología avanza con rapidez y la capacidad de disrupción de blockchain puede llegar a tener un efecto negativo, ya que los nuevos trabajos creados suelen ser de una cualificación muchísimo más elevada y, por lo tanto, resultará más difícil reciclar a los trabajadores que los perdieron por quedar estos obsoletos. Esperemos que no sea así.

Sobre este impacto real, práctico —no ya teórico o especulativo, o de cuento de la lechera—, quiero insistir en este último capítulo. Sabemos que todavía nos movemos en terrenos emergentes, muy poco maduros, y que tenemos muchas tareas por hacer, comenzando por otorgarle desde ya mismo un estatus o una importancia pública que demanda actuaciones por parte de nuestros reguladores, quienes deben ir asimilando la nueva realidad. Atendamos un poco a lo que se está haciendo al respecto.

EL ROL DE LOS REGULADORES

Por reguladores entendemos lógicamente las entidades que existen en cada país que se ocupan de velar por la estabilidad de los mercados y activos financieros y de proteger a los inversores minoristas. La más conocida en el mundo es la SEC —Securities and Exchange Commission—, la Comisión de Bolsa y Valores de Estados Unidos. En España tenemos la Comisión Nacional del Mercado de Valores (CNMV), en Reino Unido la FCA —Financial Conduct Authority—, en Suiza la FINMA —Financial Market Supervisory Authority—, etc. Son las encargadas de establecer las reglas de funcionamiento de los mercados financieros con el objetivo, sobre todo, y como hemos dicho, de proteger al inversor minorista, que desconoce la complejidad y riesgos de ese

tipo de productos, y evitar que sucedan cosas como, por ejemplo, el reciente caso de las preferentes en nuestro país.

Hoy por hoy, estas entidades se han de enfrentar al novedoso mundo cripto que hasta hace bien poco estaba desregulado o casi ni existía. Lo cierto es que prácticamente se ignoró al verse como un fenómeno demasiado nuevo sin apenas incidencia. Esta ha sido la actitud hasta no hace mucho, cuando se ha empezado a apreciar que se trataba de un asunto bastante más importante en el que también ha comenzado a incorporarse el inversor minorista. Podemos decir que como parte del año Netscape de cripto en 2017, también ha sido el año en que los reguladores han entrado de cabeza y han empezado a ponerse serios.

Así pues, los reguladores deben plantearse qué hacer con todo esto, y al respecto se han adoptado posiciones completamente antagónicas: desde actitudes muy agresivas y reguladoras, como en China o Corea, hasta las más permisivas y «criptófilas» como en Japón, Estados Unidos, Suiza o, últimamente, en Venezuela.

China básicamente ha llegado a prohibir la participación de sus inversores en cualquier operación de ICO, e incluso ha ordenado que se cierren cuentas bancarias asociadas con *exchanges*. Asimismo, está intentando eliminar de su país a los mineros —este era precisamente uno de los sitios con más mineros instalados, puesto que el acceso al hardware era sencillo, ya que casi todo se fabrica allí, y el consumo energético es barato—, y bloqueando el acceso a Internet en todos los aspectos cripto posibles.

La postura de China es de las más agresivas respecto a este universo, quizás también, o precisamente, porque era uno de los países donde más actividad había y, por lo tanto, más descontrol. En cualquier caso, no parece el ejemplo que se deba tener en cuenta, pues no debemos perder de vista que no se trata de un país democrático y en todos los sentidos ejerce un fuerte control, tanto sobre Internet como sobre la salida de capitales de su país, y en ambos sentidos parece obvio que la criptoeconomía representa un fuerte riesgo para esa mentalidad.

Pero sí que hay muchos países con políticas bastante restrictivas. También Corea del Sur ha prohibido las ICO —aunque los inversores coreanos sí que pueden invertir en ellas en otros países—, y no permite intercambios de criptomonedas de forma anónima: exige que se verifique la identidad de los intervinientes siempre, en cualquiera de las operaciones realizadas con monedas digitales.

En el otro extremo, y siguiendo por el continente asiático, Japón y Singapur son países más abiertos a la criptoeconomía. Japón tiene ya tradición en cuestión

de compras digitales, allí el bitcoin está muy aceptado, y es posiblemente el país del mundo donde más movimiento hay en este sentido. Por su parte, en Singapur, muy vinculado a la innovación, también se registra mucha actividad cripto, y su entidad reguladora, el MAS —Monetary Authority of Singapore—se muestra muy benevolente, y aunque tiende a emitir informaciones alertando de los posibles riesgos y estafas, en ningún caso trata de prohibir o intenta parar la extensión de esta nueva realidad.

Respecto a Occidente, los reguladores en general han sido últimamente proactivos, pero con actitud abierta y permisiva. La SEC en Estados Unidos suele emitir notas de advertencia de manera constante, demostrando que por un lado asumen que se trata de un tema con mucho futuro y ciertamente innovador, y que es muy posible que la nueva economía termine por estar basada en blockchain y criptomonedas; pero, por otro lado, se muestran estrictos con respecto a las leyes vigentes. Por ejemplo, permanecen atentos a las emisiones de tokens: quienes quieran emprender esta operación deben ajustarse estrictamente a la legislación vigente que afecta a los mercados de valores y bolsa tradicionales.

Podemos afirmar que, en general, Estados Unidos mantiene una postura positiva consistente en regular, pero sin prohibir, y no impedir el crecimiento de la criptoeconomía. Incluso recientemente el jefe de la CFTC —CommoditiesFutures Trading Commission—, Christopher Giancarlo, se ha convertido en una pequeña celebridad en el mundo cripto con sus comentarios muy favorables sobre blockchain y cripto y su compromiso en regular de forma cuidadosa para respetar el interés que las nuevas generaciones —los llamados *millennials*— tienen en estas tecnologías. Esta es, en general, la actitud habitual de los países occidentales, lo cual es positivo.

En Europa, donde se ha regulado con mayor atención todo esto es en Suiza, pero con vocación francamente abierta al universo cripto. Hablamos de un país donde, como es bien sabido, siempre se ha mantenido una gran apertura hacia todas las posibilidades que puede ofrecer el sector bancario y financiero, y ahora también busca establecerse como una especie de primera nación cripto en el terreno financiero, siendo el país que reúna las principales operaciones de ICO, por ejemplo, sin comprometer, obviamente, sus habituales estándares de integridad y de protección al inversor minorista de los mercados financieros existentes.

Suiza se encuentra inmersa ahora en pleno proceso regulador, poniendo especial atención a la verificación de la identidad de los inversores para evitar

estafas o blanqueo de dinero. Se trata seguramente del país que mejor y de forma más positiva y abierta hacia lo cripto se está posicionando. Esto provoca que se esté ya mirando mucho hacia Suiza a la hora de llevar a cabo ICO y trabajar dentro de este universo. Incluso el propio ministro de Economía suizo, Johann Schneider-Ammann, ha declarado que quiere que Suiza sea la primera nación cripto del mundo. Todo ello tiene también un valor, si queremos, simbólico: lo que hace el país referente de la actividad financiera puede verse como un reconocimiento a que la criptoeconomía está tirando para adelante.

En España, la CNMV básicamente está replicando lo que se dice desde el Banco Central Europeo, y que se corresponde con una actitud de cierta prudencia y cuidado, muy alerta de los riesgos que existen, de que se está viviendo una burbuja especulativa, y de que se están manejando inversiones muy poco seguras. Se focaliza la atención en la falta de seguridad de las operaciones de compra de las ICO, que tienen alta probabilidad de fracaso.

En este punto yo quisiera matizar que al fin y al cabo esto no es un problema de la fórmula de las ICO, sino de la propia naturaleza del activo en que se invierte, ya que por definición la financiación de una start-up o un negocio nuevo y emergente ha de ser arriesgada y muchas de ellas van a fallar. Cuando oigo que alguien dice que el 90 % de las ICO fallarán, siempre pienso que es lo normal, pues esa es la tasa de mortalidad que tienen las start-ups en general para un inversor de capital riesgo.

Resulta interesante citar por último el caso de Venezuela, un país que tuvo una actitud muy cerrada hacia la criptoeconomía, pero que ha cambiado radicalmente su postura. Hay que tener en cuenta que allí padecen de un grave problema de inflación con su moneda nacional, y una criptodivisa les ofrece alternativas interesantes. Además, su electricidad es muy barata, lo cual favorece que prolifere gente haciendo minado. Por eso quieren regular esta práctica de la minería, pero sin prohibirla, y han llegado a hacer algo realmente pionero, aunque no exento de polémica: han emitido la primera criptomoneda por parte de un Estado: el petro, que se vincula al precio de un barril de petróleo.

El petro, la primera criptomoneda emitida por un Estado

A principios de diciembre de 2017, el mundo cripto amaneció con una inesperada noticia: Nicolás Maduro, el presidente de Venezuela, un país en plena crisis económica y con una moneda, el bolívar, en plena espiral de devaluación y pérdida de valor, anunciaba la creación de una

criptomoneda llamada petro sustentada por barriles de petróleo, y que según el gobierno venezolano les iba a permitir salir de la crisis e intentar resolver «el bloqueo» financiero que sufre el país.

La crisis en Venezuela, acompañada de los bajos precios de la electricidad, ya había convertido el minado de Bitcoin en una actividad bastante popular. Como te podrás imaginar, el anuncio no estuvo exento de polémica y controversia, ya que mucha gente, y otros gobiernos, pusieron en duda desde el primer momento las bondades de esta criptomoneda, y expresaron su desconfianza hacia la capacidad del gobierno venezolano —que digamos que no cuenta con la mejor fama del mundo en política monetaria con el bolívar, o en transparencia sobre su gestión—, para administrar la criptomoneda y mantener, realmente, las reservas de petróleo a las que se referían para sustentarla.

El objetivo era lanzar un total de 100 millones de petros y que estos alcanzaran un valor en el mercado de 6000 millones de dólares. La oposición venezolana ha expresado su oposición al polémico proyecto y ha anunciado que si Maduro pierde las elecciones declararán el petro como ilegal. A pesar de todo, el gobierno ha seguido adelante con su proyecto, y recientemente ha declarado una confusa y poco transparente preventa de las primeras emisiones del petro por un valor cercano a los 800 millones de dólares. Pero, en fin, será el futuro el que nos diga si este experimento es legítimo y si en realidad ha de servir para sacar a Venezuela de su crisis.

Lo que hace Venezuela es apartar una reserva de petróleo y emitir su criptomoneda sobre esa base. Y lo cierto es que han recaudado una cantidad nada desdeñable con la emisión de su petro. Aunque como muchas cosas en ese país, la ICO del petro no ha estado exento de polémica: desde el cambio de última hora de la plataforma de Ethereum a NEM para la emisión del mismo, a las acusaciones que se están vertiendo desde Internet de que en realidad no han recaudado todo lo que dicen con su ICO, o a la falta de transparencia sobre el proceso, lo cual no deja de ser el *modus operandi* habitual en ese país.

En cualquier caso, esta iniciativa no deja de tratarse de algo todavía muy experimental y bastante sofisticado, porque exige toda una estructura de minado detrás a nivel nacional. En Venezuela incluso han nombrado desde el gobierno un responsable máximo llamado Carlos Vargas para que lo gestione y regule.

Tengamos en cuenta que, además, el petro cuenta con un activo detrás —el petróleo— que lo respalda, y por eso está abriendo una nueva vía que ataja precisamente uno de los problemas de las criptodivisas, su volatilidad, tal y como ya hemos explicado.

Lo cierto es que ya ha habido varios países —Reino Unido o Estonia, por ejemplo— que han mostrado su interés por contar con una criptomoneda que se base en monedas ya existentes como la libra o el dólar, o en emitir una nacional nueva, pero como criptomoneda. Es evidente que esto atenta contra la filosofía más maximalista del bitcoin, que nació con el propósito de desintermediar y prescindir de gobiernos centrales, y aquí nos encontramos con el hecho de que serían los propios gobiernos quienes emitieran las monedas digitales. Por otro lado, también es cierto que el uso de criptomonedas respaldadas por gobiernos las dotaría de una legitimidad importante, y haría que la adopción por parte de la población fuera muchísimo más rápida. Yo creo que ayudaría también al crecimiento de las verdaderas criptomonedas descentralizadas como el bitcoin.

Supongo que el hecho de que se alce hacia las autoridades una demanda por la regulación quizás pueda apreciarse como una paradoja en algo que nació con vocación descentralizadora y como respuesta precisamente a las actuaciones de los gobiernos y los bancos. Pero no se trata de atentar contra la filosofía identitaria del universo cripto, sino de asumir que la extensión y potencial impacto del mismo es ya global.

¿Ventajas fiscales para las empresas de blockchain en España?

A primeros de este año 2018 se anunció en prensa que el Partido Popular estaba preparando un proyecto de ley para ofrecer posibles desgravaciones fiscales a las compañías de blockchain o a las que se financiaran mediante ICO como incentivo para atraer a este tipo de empresas a nuestro país.

Según fuentes del partido del gobierno, quieren crear las condiciones adecuadas para que España sea líder en el origen de criptomonedas. Asimismo, por otro lado, se han avisado de los riesgos que conllevan

las mismas por el componente especulativo con el que de momento están siendo utilizadas.

El encargado de redactar el proyecto es Teodoro García Egea, portavoz adjunto de la Comisión de Energía, Turismo y Agenda Digital del Partido Popular, y ha asegurado que es importante que se dé la bienvenida a blockchain como tecnología que podría impulsar la innovación en sectores como las finanzas, la salud y la educación. Según Teodoro García, lo que se busca es «establecer el marco más seguro de Europa para invertir en ICO».

IMPACTOS FINANCIEROS, IMPACTOS GLOBALES

Termino ya. Pero subrayando una vez más la importancia del impacto que la criptoeconomía comienza a tener en nuestro mundo, y de sus previsibles efectos en distintos ámbitos.

Todo lo que acabamos de ver, llegando al punto incluso de ser testigos de que los propios gobiernos se muestran interesados en crear monedas digitales —lo cual rompe por completo, como hemos dicho, con la filosofía de partida del bitcoin—, no es sino una significativa muestra de cómo se expanden las posibilidades y el potencial del universo cripto.

Existen ya, como sabemos, diferentes posibilidades de empleo de criptomonedas y blockchains, una oferta tan amplia que permite que cada cual pueda adaptarlo a su filosofía y principios. Pero la revolución tecnológica es global, y nuestra organización social no puede menos que contemplarlo. Estamos haciendo camino y debemos aprovechar las oportunidades a todos los niveles.

Bitcoin fue el punto de partida y nos presentó una «magia tecnológica» detrás, la del blockchain, llamada a disrumpir poderosamente los mercados financieros.

Después, la tecnología mejorada que nos ofrecía Ethereum se ha destapado como mucho más potente que lo visto hasta el momento, y su contribución a la criptoeconomía está llamada a ser francamente revolucionaria, puesto que, como decíamos, sobrepasa el ámbito estricto del dinero digital y entra de lleno en el concepto de propiedad digitalizada, que abre muchísimas y nuevas posibilidades en los mercados, ofreciendo innovadoras maneras de financiar y monetizar proyectos empresariales, así como vías poderosas para proporcionar liquidez.

Otros ejemplos significativos del proceso de transformación que estamos viviendo se comenzaban a gestar en 2016, cuando se creaba un nuevo producto dentro de la red de Ethereum: un mercado predictivo llamado Augur que se convertía en una de las primeras apps descentralizadas que emiten tokens por encima de Ethereum. Estoy convencido de que el futuro es de estas apps descentralizadas que interactúan con la blockchain de Ethereum y que son desarrolladas no de forma centralizada por una empresa, sino en muchos casos por un grupo de desarrolladores en código abierto.

El hecho de que se pueda emitir fácilmente un token que va a tener una utilidad dentro de una plataforma descentralizada creada por encima de Ethereum, y que lo puedas prevender al público mediante *crowdfunding* y así financiar el desarrollo, hace que surjan iniciativas de *Dapps* que se pueden convertir en las aplicaciones del futuro. Las *Dapps* o aplicaciones distribuidas prometen también plantear retos a los actores dominantes de Internet de hoy, que están altamente centralizados.

Todo esto está ocurriendo en buena medida gracias a la popularización de los contratos inteligentes y de las ICO, que se están extendiendo a ritmo exponencial en infinidad de actividades de carácter financiero o empresarial.

El futuro de las ICO es un tema especialmente interesante. Desde que el conocido emprendedor del mundo cripto y *chairman* de la Bitcoin Foundation, Brock Pierce, lanzara el primer ICO en 2013 con la criptomoneda Namecoin y consiguiera captar cinco millones de dólares en bitcoin, el mundo de las ICO ha ido creciendo de forma paulatina hasta la gran explosión que ha tenido en 2017, el año Netscape de la criptoeconomía. Sin embargo, todavía es muy pequeño: como ya hemos dicho equivale a menos del 10 % de la financiación por *crowdfunding*, y a menos del 1 % de la financiación por capital riesgo. Está todavía comenzando, aunque ya se intuya que lo que ha explotado con tal fuerza con las primeras ICO, y lo mucho que han recaudado, no va a volver a ocurrir. Ha sido una explosión que ha favorecido los «pelotazos», pero no es probable que ocurra con frecuencia.

Aunque las ICO sí que van a continuar. Como apuntábamos antes, los reguladores cada vez habrán de ser más proactivos a la hora de regular estos temas. En todo caso, esta previsible regulación venidera creo que va a resultar positiva, que va a traer orden y que va a limitar las posibilidades de los estafadores. Lo que va a cambiar realmente es que el dinero más tradicional de capital riesgo y otros inversores empiece a apostar por este mundo que de momento sigue muy copado por los entusiastas habituales y los pioneros del

cripto, cuyos activos se han revalorado muchísimo. Entrará más dinero y se irá incrementando su magnitud. Tiempo al tiempo. Por supuesto que hay que solucionar algunos problemas —ya los hemos ido desgranando— y es necesario que las cosas se hagan de forma más ordenada, que surjan nuevos roles vinculados a la criptoeconomía, como el de los custodios, intermediarios que almacenen los tokens o las criptomonedas, es decir, garantes de que el dinero no se pierda, que se conserven de forma segura las claves de los monederos, entre otras cosas. Esto puede ser importante para que entre en mayor medida el dinero institucional dentro del mundo de las ICO.

Y está también todo lo relativo a la propiedad digital y la tokenización de activos de la que hablábamos al final de la segunda parte de este libro. Aquí reside un potencial económico de primera magnitud. Cuando los activos pueden ser transformados en títulos digitales, las posibilidades en diversos mercados —como el financiero, el inmobiliario, el de infraestructuras o el del arte— son infinitas. Estamos hablando de una forma de financiación alternativa realmente muy potente que no se ciñe ya solo a las start-ups, sino que se extiende también a grandes proyectos inmobiliarios, de infraestructuras, etc.

Un mercado enorme donde hay toda una revolución posible por delante. El mercado de los token sustentados por activos —o la tokenización de títulos o valores— es precisamente el foco de mi actividad en la actualidad, habiendo desarrollado la que de momento es la plataforma líder para la tokenización de estos activos, Securitize, así como el fondo de capital riesgo tokenizado más grande del mundo, SPiCE VC. Aunque este mercado está aún inmaduro —el token de SPiCE VC ha sido el tercer *security token* en ser emitido en el mundo en marzo de 2018, para que te hagas a la idea—, todo apunta a que durante 2018 va a tener un crecimiento tremendo, y en 2019 superará a los más tradicionales *utility tokens* que han dominado hasta ahora.

Como hemos visto, incluso los gobiernos se muestran interesados en emitir monedas digitales, lo cual es sintomático. Se abren nuevas posibilidades, que, además, ya no son estrictamente cripto, pero que sí aportan otras formas de usabilidad. Queda todavía por verse el posible impacto de esto en el uso efectivo de las criptomonedas para intercambios comerciales. Mi visión personal es que va a suceder algo similar a lo que ya ocurrió en el mundo de las telecomunicaciones, en el que, como he dicho, trabajé durante diez años y en el que fui testigo de las transformaciones que la digitalización trajo consigo.

Ya hemos visto que, en realidad, WhatsApp o Skype no han hecho que desaparezca la llamada de voz o la mensajería como servicio de las empresas de

telecomunicaciones; lo que han hecho es reducirla a otra alternativa más y marcar presión sobre el precio. Esto fue muy impactante en un mercado oligopólico tan regulado, con tantas barreras de entrada y con tan pocos agentes operando por país. El sector financiero es similar en esos aspectos.

El universo cripto hace vislumbrar muchas alternativas, que todavía hoy por hoy no funcionan igual de bien, que requieren de tiempo, pero a medida que vaya madurando y se facilite el uso, no es que vayan a provocar que los bancos —o los mismos bancos centrales— desaparezcan, pero sí que exista una presión para que se comporten de una forma más adecuada y se abaraten costes cuando se compruebe que desde el mundo cripto se pueden hacer cosas muy baratas y sin coste por los servicios que ahora te cobran un buen dinero. Del mismo modo que WhatsApp y Skype facilitaron que bajaran los precios de las llamadas de voz y los SMS.

Los bancos van a tener que espabilar para hacer las cosas de manera más eficiente, van a tener que digitalizarse más, y ellos mismos terminarán introduciendo la propia tecnología de blockchain en sus procesos, como ya están haciendo de la mano de empresas como Ripple. También van a tener que empezar a comportarse de manera más transparente y respetuosa con los ciudadanos.

Por supuesto, otros ámbitos laborales se verán también afectados: visiblemente abogados y notarios, ya que son profesionales que intermedian con el activo de la confianza, y la nueva tecnología se erige ahora como un gran tercero en credulidad. Pero también cualquier otro trabajo que exija lo mismo.

En definitiva, estamos aquí refiriéndonos a tecnologías muy disruptivas que van a transformar muchísimas industrias, y esos efectos no solo se van a apreciar en la actividad empresarial, sino también en nuestras vidas cotidianas. Como ya hemos repetido varias veces, estamos todavía en un momento de efervescencia que está emergiendo con cierta inmadurez, y falta mucho camino técnico, de negocio, de regulación, por recorrer. Así que en realidad está todo por hacer, pero eso también lo convierte en más emocionante e, intelectualmente, más retador.

EPÍLOGO

UN FUTURO DESCENTRALIZADO

Nos encaminamos hacia un futuro descentralizado.

Cuando Internet empezó en los años ochenta y noventa, funcionaba con protocolos abiertos controlados por la comunidad de Internet. Las personas y organizaciones que querían participar sabían cuáles eran las normas de funcionamiento, podían crear sus propios servidores instalándose software de código abierto y hasta podías tener tu propio servidor de correo electrónico. La promesa de Internet consistía, básicamente, en eso; en lo que anticipaba Milton Friedman: una red abierta y descentralizada, sobre la que se llegó a especular incluso que habría de sustituir a los gobiernos.

Obviamente eso no ha ocurrido y, en verdad, lo que ha pasado desde entonces es que las empresas que se han hecho más fuertes en Internet, las que conocemos como GAFA —Google, Amazon, Facebook, Apple—, han construido cosas tan útiles —buscadores, correo electrónico, dispositivos móviles, comercio electrónico, redes sociales, servicios en la nube, etc.— que la gente ha ido migrando de servicios abiertos y descentralizados a los centralizados de estas empresas, puesto que son más potentes y sofisticados.

Se ha perdido el espíritu original de Internet como red descentralizada de protocolos abiertos en la que no había intermediarios. Internet se convirtió en todo lo contrario, en una red centralizada y, además, controlada por unos pocos agentes. Ese entusiasmo inicial por desintermediar los actores principales y los gobiernos no solo no se ha cumplido, sino que se ha acentuado lo contrario. Se ha movido la cadena de valor, se ha progresado técnicamente y hay nuevos servicios, pero el control se ha movido de unas manos a otras.

Ahora mismo, aquel espíritu original descentralizador se está volviendo a vivir en el universo cripto y blockchain. Los impulsores son en buena medida los mismos que en los inicios de Internet —personas de espíritu libertario—, que

creen en la promesa de aquella idea original de que la red sea algo descentralizado en manos de la comunidad de usuarios. Ese es el gran entusiasmo existente alrededor de esta industria.

Es ya famosa la ley de Johnston —formulada inicialmente en 2014 por David Johnston, uno de los primeros inversores en criptomonedas, protocolos y aplicaciones descentralizadas— que dice que «lo que se pueda descentralizar se va a descentralizar». Claro que puede volver a pasar lo mismo si las criptomonedas se terminan centralizando como ya sucede con el caso de Ripple, pero la expectativa es otra: la descentralización definitiva. Si puede funcionar es porque al principio los protocolos abiertos estaban en manos de organizaciones sin ánimo de lucro, y por eso las que sí lo tenían pronto tuvieron más recursos para invertir y mejorar los protocolos, y para ofrecer mejores servicios captando así a los usuarios.

Sin embargo, ahora los incentivos económicos existentes en las redes cripto —la minería, los tokens…— incentivan la participación y permiten monetizar al nivel del protocolo —tal y como ocurre con Bitcoin como ejemplo paradigmático—, todo lo cual hace pensar que la gente que participa en estas redes distribuidas va a tener más fuerza que las compañías que en su día concentraron el dominio en la capa de la aplicación. Esto es lo que se conoce como *fat protocols* o protocolos gruesos, término introducido por el inversor Joel Monegro.

Por eso estamos ante una nueva era de Internet: la era del valor. La transmisión de valor y de confianza existe gracias a estos nuevos protocolos. Y, además, ha venido acompañada de unas posibilidades de monetarización que hace que el concepto de descentralización y los protocoles sean mucho más potentes.

Yo no me adscribo a una postura libertaria ni anarquista, y creo que debe existir una regulación que ponga orden a esto. Tampoco digo que el bitcoin sea la panacea ni la solución a todos los problemas. Pero es patente que lo vivido en los últimos años ha demostrado que existen fuertes deficiencias en las políticas monetarias globales, y que los roles de los gobiernos y los agentes financieros resultan bastante cuestionables. Blockchain es una tecnología esperanzadora porque es evidente que la centralización ha fallado y que las alternativas descentralizadas, cuando maduren —mayor escalabilidad, estabilidad y sostenibilidad— pueden llegar a reemplazar a las centralizadas.

Christine Lagarde, la máxima responsable del Fondo Monetario Internacional, una de las instituciones financieras más influyentes que existe en el mundo, dijo

recientemente que las criptomonedas pueden llegar a reemplazar un día a las monedas existentes y las políticas monetarias centrales, y que la mejor respuesta que los bancos centrales podían tener era intentar continuar gestionando políticas monetarias eficientes a la vez que estar abiertos a nuevas ideas y nuevas demandas de la sociedad. Al mismo tiempo que nuestra economía evoluciona. No puedo estar más de acuerdo.

Contar ahora mismo con miles de desarrolladores descentralizados que reciben incentivos por operar con códigos abiertos es, sin duda, un gran beneficio para la sociedad, que va a permitir a los usuarios elegir las infraestructuras financieras que sirvan mejor a sus intereses.

La criptoeconomía permite la nueva Internet del valor y un futuro descentralizado. La descentralización, como vemos, ha llegado para quedarse. Si esto pasa, se conseguirá de verdad reducir el rol de los gobiernos y de las grandes empresas como Internet prometía hacer en su momento. Un cambio que necesariamente ha de ser un proceso democratizador.

Pero como terminaba el capítulo anterior, todavía está todo por hacer, y eso es emocionante, además de un reto. Es el momento de apostar por ello.

BIBLIOGRAFÍA

ANTONOPOULOS, ANDREAS M., *The Internet of Money,* 2016.

BURSNISKE, CHRIS yTATAR, JACK, *Cryptosassets: the innovative investor's guide to bitcoin and beyond,* 2017.

BUTERIN, VITALIK *et al.,* «Ethereum whitepaper (2013+): A Next-Generation Smart Contract and Decentralized Application Platform», https://github.com/ethereum/wiki/wiki/White-Paper.

DIXON, CHRIS, «Crypto tokens: A breakthrough in open network design», https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef. 2017.

GRIGG, IAN, «Seeking consensus on consensus - DPOS (delegated proof of stake) and the Two Generals' problem», https://steemit.com/eos/@iang/seeking-consensus-on-consensus-dpos-or-delegated-proof-of-stake-and-the-two-generals-problem.

JOHNSTON,DAVID A., «Everything Will Be Decentralized», https://medium.com/@DJohnstonEC/everything-will-be-decentralized-d7dcedca45e. 2014.

KASIREDDY, PREETHI, «Blockchains don't scale - not today, at least… but there's hope», https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a. 2017.

LAMPORT, LESLIE *et al.,* «The Byzantine Generals Problem», https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf, 1982.

MONEGRO, JOEL, «Fat protocols», https://www.usv.com/blog/fat-protocols. 2016.

NAKAMOTO, SATOSHI, «Bitcoin whitepaper: A Peer-to-Peer Electronic Cash System», https://bitcoin.org/bitcoin.pdf, 2009.

PETKANICS, DOUG, «Inflation and participation in stake based token protocols», https://medium.com/@petkanics/inflation-and-participation-in-stake-based-token-protocols-1593688612bf. 2017.

POPPER, NATHANIEL, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money,* 2016.

ROUX, YANNICK, «Reflections on proof of work energy consumption», Token Economy Newsletter, 26, https://tokeneconomy.co/token-economy-26-reflections-on-pow-energy-consumption-cryptokitties-erc-721-tokens-1e6e2ea3d413. 2017.

RUSSELL, RUSTY, «The Three Economic Eras of Bitcoin», https://medium.com/@rusty_lightning/the-three-economic-eras-of-bitcoin-d43bf0cf058a, 2017.

SNIDER, MYLES, «An overview of stablecoins», https://multicoin.capital/2018/01/17/an-overview-of-stablecoin. 2018.

SRINIVASAN, BALAJI, «Thoughts on tokens», https://news.earn.com/thoughts-on-tokens-436109aabcbe. 2017.

STARK, ELIZABETH, «What is the Lightning Network and how can it help bitcoin scale?», https://coincenter.org/entry/what-is-the-lightning-network. 2016.

STARK, JOSH, «Digital collectibles and the weird future of "digibles"», https://hackernoon.com/digital-collectibles-and-the-weird-future-of-digibles-f75f4bf0f9aa. 2017.

SZABO, NICK, «The idea of smart contracts», http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2 1997.

VIGNA, PAUL yCASEY, MICHAELJ., *Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order,* 2015.

VIGNA, PAUL yCASEY, MICHAEL J., *The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order,* 2016.
WENGER, ALBERT, «Crypto tokens and the coming age of protocol innovation», http://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol.

Tolo lo que querías saber sobre bitcoin, criptomonedas y blockchain y no te atrevías a pruguntar
Carlos Domingo

Diseño de la cubierta: Jose Luis Paniagua
Fotografía de la solapa cortesía del autor

Ediciones Temas de Hoy es un sello editorial sello editorial de Editorial Planeta, S. A.
Avda/ Diagonal, 662-664, 08034 Barcelona (España)
www.planetadelibros.com

Primera edición en libro electrónico (epub): mayo de 2018

ISBN: 978-84-9998-671-5 (epub)

Conversión a libro electrónico: Safekat, S. L.
www.safekat.com

¡Encuentra aquí tu próxima lectura!

¡Síguenos en redes sociales!